eCH-0107 Principes de conception pour la gestion de l'identité et de l'accès (IAM)

Nom	Principes de conception pour la gestion de l'identité et de l'accès (IAM)
eCH-nombre	eCH-0107
Catégorie	Norme
Stade	implémenté
Version	3.0
Statut	approuvé
Date de décision	2018-11-28
Date de publication	2019-02-07
Remplace version	2.0 <Major Change>
Condition préalable	-
Annexes	-
Langues	Allemand (original), français (traduction)
Auteurs	Groupe spécialisé IAM Groupe de projet SEAC Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch Marc Kunz, BFH TI, marc.kunz@bfh.ch Thomas Kessler, Temet, thomas.kessler@temet.ch Torsten Gruoner, UPIC, torsten.gruoner@isb.admin.ch Marc Heerkens, UPIC, marc.heerkens@isb.admin.ch Groupe spécialisé eCH IAM
Éditeur / Distribution	Association eCH, Mainaustrasse 30, case postale, 8034 Zurich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

Le présent document définit les principes, les règles et les cadres réglementaires relatifs à la conception du système IAM, devant être pris en compte dans le cadre de la mise à disposition des solutions IAM fédératives dans la cyberadministration Suisse. Le principe de conception définit un paysage IAM modèle pour les scénarios d'application inter-organisationnels pour les applications existantes et nouvelles en partant du principe que les processus et les services IAM peuvent être motivés par les exigences des différentes Stakeholders et fournis et utilisés par les acteurs définis. La norme spécifie les exigences, les Stakeholders et les acteurs, les processus, l'architecture de l'information et les services IAM. Y sont également abordés les aspects de la protection de la sphère privée et les répercussions de l'expansion de l'IAM à l'Internet of Things.
La norme peut être utilisée dans tous les domaines de l'eSociety (cyberadministration, E-Health, E-Economy).

Table des matières

Remarque

En vue d'une meilleure lisibilité et compréhension, seul le genre masculin est utilisé pour la désignation des personnes dans le présent document. Cette formulation s'applique également aux femmes dans leurs fonctions respectives.

1 Statut du document

***Approuvé**:* Le document a été approuvé par le comité d'experts. Il a pouvoir normatif pour le domaine d'utilisation défini dans le domaine de validité donné.

2 Introduction

2.1 Vue d'ensemble

Au cours des dernières années, l'utilisation d'internet s'est accrue de manière constante. Internet est de plus en plus fréquemment utilisé, non seulement en tant que source d'information, mais également pour réaliser des affaires.

Les processus administratifs en ligne présupposent des sujets dignes de confiance et donc une entente avec les partenaires administratifs. Le service de gestion de l'identité et de l'accès (Identity and Access Management, IAM) interne à l'organisation a jusqu'à présent garanti des services administratifs adaptés. Les scénarios d'utilisation inter-organisationnels montrent les limites de l'IAM interne. En effet, des dépenses considérables sont nécessaires pour qu'il puisse être utilisé par plusieurs *domaines*. La présente norme définit les exigences et les principes de base pour la conception *de systèmes IAM fédérés* (également appelés systèmes IAM ou système IAM global dans le document), afin que la limite mentionnée ci-dessus puisse être surmontée. Ces principes doivent être pris en compte lors de la préparation de solutions destinées à la cyberadministration suisse, afin que les applications et les services locaux puissent être utilisés par toutes les organisations. La norme sert de base pour toutes les personnes qui élaborent des solutions destinées à un environnement de cyberadministration, potentiellement ou déjà préparé pour un externe (Internet-eServices).

Dans un environnement de cyberadministration, il s'agit, comme dans le contexte global de l'E-Society (cyberadministration, E-Health, E-Economy), du principe selon lequel des *sujets* (administrations, citoyens, organisations, entreprises, applications spécifiques) souhaitent utiliser des ressources (services des municipalités, des cantons, de la confédération ou d'un tiers). Le défi majeur réside dans le fait que les *E-ressources* et les *E-Identities* puissent se trouver dans des *domaines* différents.

2.1.1 Introduction IAM

Les éléments clé d'un *IAM* sont essentiels pour comprendre la norme et sont donc brièvement expliqués dans ce paragraphe. La terminologie employée dans ce document est tirée du glossaire IAM (eCH-0219 [1]) et est indiquée en italique.

La Figure 1 ci-dessous illustre les éléments-clé de l'IAM. Cet IAM se concentre avant tout sur l'accès contrôlé d'un *sujet* à une *ressource digne* d'être protégée.

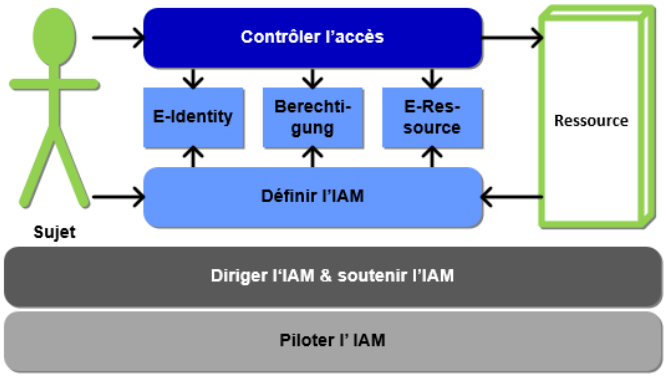


Figure 1 Vue d'ensemble de l'IAM

Les éléments *Contrôler l'accès* et *Définir l'IAM* constituent les processus centraux qui sont utilisés par le *sujet* et le *Relying Party*. Ces processus centraux sont utilisés à des moments différents, symbolisés par la couleur bleu clair et bleu foncé (utilisation des couleurs voir Tableau 1).

gris clair	Dans ce document, la couleur gris clair sert à visualiser les éléments, qui ont le caractère de standardisation et proposent ou définissent des garde-fous
gris foncé	Dans ce document, la couleur gris foncé sert à visualiser les éléments déjà actifs avant la *période de définition* et durant toute la durée de vie du système IAM (processus d'appui comme la gestion ou le soutien par exemple).
bleu clair	Dans ce document, la couleur bleu clair est utilisée exclusivement pour la *période de définition* au cours de laquelle toutes les informations des éléments d'information sont classées (c.-à-d. définies).
bleu foncé	La couleur bleu foncé est systématiquement utilisée pour la *période d'exécution*. L'accès basé sur les éléments d'information définis est contrôlé (accordé ou refusé) pendant la période d'exécution.
vert clair	Dans ce document, la couleur vert clair est exclusivement utilisée pour les objets du monde réel.

Tableau 1 Utilisation des couleurs dans le document

Le *sujet* et la *ressource* sont des objets du monde réel qui atteignent leurs objectifs au moyen de processus IAM. Le *sujet* a pour objectif d'accéder à la *ressource* souhaitée. La *ressource* a pour objectif de protéger ses ressources contre tout accès non-autorisé aux informations et aux services.

Des illustrations numériques – on parle également d'éléments d'information - sont attribuées aux objets du monde réel (*sujet, ressource*), afin que les processus principaux puissent aussi fonctionner dans l'univers numérique. L'*E-Identity* (bleu clair) est attribuée au *sujet* (vert), et l'*E-Ressource* (bleu clair) est attribuée à la *ressource* (vert). Afin de réaliser ses objectifs, le *Relying Party* définit dans l'élément d'information *Autorisation* (*règles d'entrée/droit d'accès*) quelle *E-Identity* peut avoir accès à quelle *ressource* et sous quelles conditions.

Le processus *Réguler l'IAM* couvre l'ensemble des activités relatives à la définition des exigences et des conditions générales. Le processus *Diriger & soutenir l'IAM* englobe le Direction de la mise en œuvre et de l'exploitation d'un système IAM, ainsi que les activités destinées à prendre en compte, gérer, suivre et, au final, résoudre les problèmes (Support).

2.1.2 Champ d'application

La vision de l'administration interconnectée et des processus globaux en résultant dans la cyberadministration suisse nécessite une *gestion de l'identité et des accès* inter-organisations. La présente norme eCH-0107 constitue la base de la standardisation IAM. Elle décrit les définitions et la terminologie tirée de eCH-0122 [2] sur lesquelles repose l'architecture de la cyberadministration suisse décrit.

La norme eCH-0107 définit les principes, les exigences, les processus et les services IAM pour la conception du système IAM devant être pris en compte lors de la mise en place de solutions IAM inter-organisationnelles, dans la cyberadministration fédérale suisse, de sorte à ce que les applications locales puissent être utilisées indépendamment des organisations.

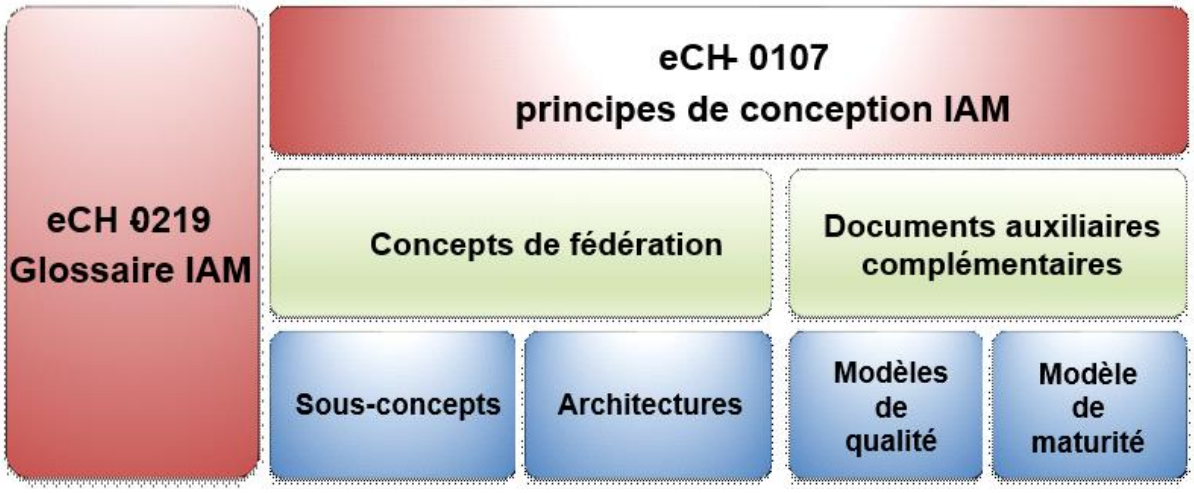


Figure 2 Classement de la norme eCH-0107

Les concepts pour les solutions IAM fédérées et les ressources supplémentaires se positionnent sous la norme eCH-0107. Le glossaire IAM (eCH-0219 [1]) définit les termes valables pour tous les standards eCH dans le domaine de l'IAM. Les concepts sont des descriptions concrètes de la forme que doit avoir une proposition de solution IAM et contiennent des sous-cadres et architectures devant être pris en compte pour la mise en œuvre. Par ailleurs, des ressources sont proposées aux concepts, mettant des informations complémentaires à disposition et qui sont pertinentes pour plus d'un concept. Les modèles de qualité et de maturité représentés sont des exemples de ressources et ne sont pas définitifs.

2.1.3 IAM fédéré

Contrairement à l'IAM interne à l'organisation, l'*IAM fédéré* part d'*E-Identities* inter-organisationnelles et de leur utilisation entre ces organisations.

L'*E-Identity* d'un *sujet* est établie dans le *domaine* A, mais peut également comporter des informations d'un *domaine* B et peut être utilisée pour accéder aux ressources d'un *domaine* C.

Afin de pouvoir établir un *IAM fédéré*, les différents *domaines* doivent se faire mutuellement confiance concernant des points précis. Cette confiance s'appuie sur des accords implicites et explicites.

Dans le cas de l'*IAM fédéré*, contrairement à l'IAM réplicatif (voir eCH-0219 eCH-0219 [1]), les autorités dans la cyberadministration mettent des ressources à la disposition des sujets de leurs partenaires internes (autres autorités suisses) ou externes (personnes, sociétés, organisations ou autorités d'autres Etats), servant à rendre disponibles en ligne les prestations définies dans leur domaine de compétence. Ces ressources devraient être accessibles aux sujets de leur(s) propre(s) domaine(s) et aux sujets avec des E-Identities d'autres domaines. Une autorité peut ainsi être un Relying Party mais aussi, dans certaines circonstances, également un prestataire de services IAM.

2.1.4 Délimitation

Les principes de conception et les règles figurant dans cette norme constituent le cadre réglementaire des *systèmes IAM fédéraux*. Les éléments principaux (processus et services IAM) et les *Stakeholders* et *acteurs* les plus importants y seront cités et expliqués. Les différentes typologies de systèmes IAM fédéraux seront également introduites dans cette norme. L'orchestration et la mise en œuvre concrète des propositions de solutions sont toutefois thématisées dans les concepts et ne seront pas prises en compte dans cette norme.

De manière générale, ce document prend uniquement en compte les systèmes IAM, qui contrôlent l'*accès* aux **ressources dignes de protection**. L'*accès* aux *ressources publiques* ou *cachées* n'est pas traité dans cette norme.

Le terme *E-Identity* utilisé dans la norme se réfère non seulement à l'*identité électronique reconnue par l'Etat* (*E-ID*) de la Suisse, mais couvre également l'ensemble des types d'identités électroniques habituellement utilisés à l'heure actuelle (certificats, Google-Accounts, SuisseID/SwissID par exemple). Au moment de la révision de la présente norme dans sa version 3.0, la loi e-ID[1] était en phase de consultation publique et n'a donc pas été prise en compte. Dès qu'elle entrera en vigueur, la loi e-ID et l'ordonnance correspondante devront être prises en compte lors de la mise en place et de l'exploitation d'un système IAM.

L'intégration de *systèmes IAM fédérés* entre eux – on parle d'interfédération – est seulement évoquée dans cette norme et devrait faire l'objet de sa propre norme.

L'*IAM* est l'un des moyens permettant de remplir des objectifs de sécurité majeurs. En conséquence, les solutions IAM doivent naturellement satisfaire aux exigences de sécurité en vigueur, qui sont souvent élevées. Ces exigences sont décrites dans les normes de sécurité correspondantes et ne seront pas à nouveau mentionnées dans ce document.

[1] Pour de plus amples renseignements concernant la loi e-ID, rendez-vous sur le site Web https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-id.html

2.1.5 Avantages

Des progrès considérables (déjà documentés et définis dans la deuxième version de la norme) ont été réalisés dans l'environnement *IAM* fédéré, depuis la version 1 de la norme eCH-0107. La version 3.0 élargit et corrige les affirmations de la deuxième version.

Cette norme présente les avantages suivants:

- Les éléments clé d'un *système IAM fédéré* sont connus et constituent la base afin d'élaborer les idées et propositions de solution.
- La définition d'un paysage *IAM* modèle (Stakeholders, acteurs, processus, modèle d'information, *services IAM*) dans des scénarios d'application inter-organisationnels.
- Les exigences générales imposées aux *systèmes IAM fédérés* et les exigences du Stakeholder majeur sont définies.
- Les concepts possibles pour les *Identity Federations* sont représentés.
- Les répercussions sur l'*IAM* en cas d'extension du champ d'application à l'Internet of Things sont discutées.
- Les exigences accrues en matière de protection de la sphère privée du sujet sont mentionnées.

2.2 Axes principaux

La présente norme eCH-0107 se divise en sept chapitres (en plus de l'introduction), brièvement décrits ci-dessous.

Le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.** identifie les principaux acteurs et Stakeholders ainsi que la relation qui les unit dans un *système IAM fédéré*.

Le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.** décrit les principes de base et les exigences générales imposées à un *système IAM fédéré* ainsi que les exigences de tous les Stakeholders.

Le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.** présente l'architecture de l'information et explicite les différents éléments. Les objets du monde réel relatifs à la sémantique sont affectés aux objets d'interface à l'aide de l'architecture de l'information.

Le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.** définit les processus qui importent à tous les acteurs. Cela signifie que la norme prend en compte non seulement les processus des *prestataires de service IAM*, mais également ceux du *Relying Party* et du *sujet*.

Le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.** définit les *services IAM*, dont les interfaces et le lien avec les processus sont définis dans un *système IAM fédéré*.

Le chapitre 8 les répercussions sur un système IAM, lorsque celui-ci est étendu à l'Internet of Things et que l'*authentification* et l'*autorisation* des *choses* y sont également incluses.

Le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.** décrit les exigences en matière de protection de la sphère privée du *bénéficiaire de prestations* (*sujet*), sortant du cadre des exigences stipulées à la section 4.3.1 On y trouve par ailleurs des directives concernant l'administration et le traitement des données relatives au sujet.

Le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.** expose les variantes de structure d'*IAM* fédéré.

2.3 Caractère normatif des chapitres

Les chapitres de la présente norme sont de nature soit normatifs, soit descriptifs. Le tableau ci-dessous illustre ce classement:

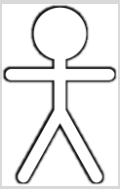
Chapitre	Description
Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	Descriptif
Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	Descriptif
Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	Normatif
Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	Normatif
Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	Normatif
Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	Les désignations et leurs définitions sont normatives. Les activités et remarques sont descriptives.
Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	La désignation et sa définition sont normatives. Les remarques sont descriptives.
Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	Normatif
Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	Descriptif
8 IAM pour l'IoT	Descriptif
Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	Descriptif

Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.	Descriptif
Annexe A – Références & bibliographie	Descriptif
Annexe B – Collaboration & vérification	Descriptif
Annexe C – Abréviations	Normatif
Annexe D – Glossaire	Normatif
Annexe F – Modifications par rapport à la version 2.00	Descriptif

Tableau 2 Vue d'ensemble du caractère normatif des chapitres

3 Acteurs et Stakeholders

Un système d'Identity & Access Management se compose de six acteurs distincts qui, en fonction de la combinaison et de l'organisation, sont motivés par cinq Stakeholders fondamentaux.

Acteurs 	Un acteur décrit la mission et le but d'une entité dans une fédération et exécute les processus. Un acteur dans un système IAM est motivé par un ou plusieurs Stakeholders.
Stakeholders 	Les Stakeholders sont des objets du monde réel, c.-à-d. des personnes, groupes de personnes ou organisations ayant des intérêts communs dans l'*IAM*. Un Stakeholder a une (ou plusieurs) attente(s) (Stakes) et a une volonté. Les Stakeholders imposent des exigences (voir chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**) aux différents acteurs dans un système IAM.

3.1 Acteurs dans l'IAM

Les différents acteurs, qui exécutent les processus (*IAM*) effectifs, sont décrits dans l'ordre alphabétique. Pour chaque acteur, on indique également le principal Stakeholder (voir chapitre 4.3).

Prestataire de services IAM	Le *prestataire de services IAM* est responsable de l'exploitation[2] d'un ou de plusieurs services IAM selon le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**. Bien que distinctes, les spécialisations illustrées par la Figure 3 sont souvent mises en œuvre conjointement.

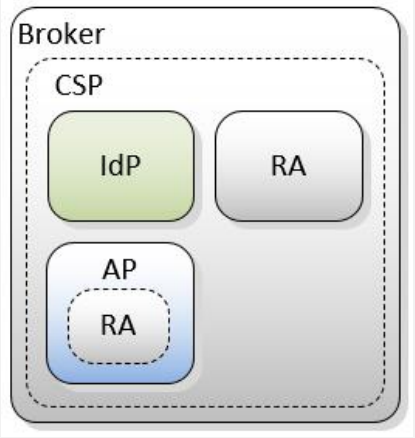


Figure 3 Prestataire de services IAM

Le *service d'inscription/Registration Authority* (*RA*) saisit et contrôle les *E-Identities* et les *attributs* des *sujets*.

L'*Identity Provider* (*IdP*) vérifie les *E-Identities* des *sujets*.

L'*Attribut Provider* (*AP*) gère les *attributs* des *sujets* et délivre des *confirmations d'attribut*.

Le *Credential Service Provider (CSP)* délivre et gère des *moyens d'authentification* pour les *E-Identities*. Un *CSP* contient toujours une *RA* et englobe les services de vérification des *E-Identities* (*IdP*).

Un *Broker* propose des services communs, comme l'administration des métadonnées, l'IdP-Discovery, l'Identity Linking ou la transformation de la *confirmation de l'authentification et de l'attribut*, pour tous les autres *prestataires de services IAM* et *Relying Parties* dans une *Identity Federation*. A titre facultatif, un *Broker* peut contenir un *CSP*.

La Figure 3 représente tous les *prestataires de services IAM*, dans le cas où ils sont mis en œuvre conjointement.

Stakeholders principaux: *prestataires de service*

[2] L'exploitation peut être assurée par le *prestataire de services IAM* lui-même ou confiée à un exploitant – on parle alors d'externalisation ou outsourcing. Dans le cas de l'outsourcing, le *prestataire de services IAM* transfère à l'exploitant les exigences qui lui ont été imposées. Ce transfert n'a aucune incidence sur le système IAM global et n'est donc pas traité de manière plus approfondie dans le présent document.

direction IAM	La *direction IAM* est en charge de la gestion d'un système IAM ou de parties de ce système (*prestataire de services IAM* ou *Relying Party*). La *direction IAM* du *système IAM global* gère les *prestataires de services IAM* et *Relying Parties* impliqués (comme pour ITIL [3] par exemple) dans tous les domaines de spécialisation, tels que Release Management, Quality Management, Gestion des fournisseurs et consommateurs IAM, Service Request Management par exemple. Ceci peut se produire aussi bien dans le contexte interne que via des contrats/SLA avec les *prestataires de services IAM* et *Relying Parties* externes. Principaux Stakeholders: *Direction*
IAM Regulator	L'*IAM Regulator* (ou *pilotage IAM*) définit les conditions générales juridiques, procédurales, organisationnelles/architecturales et techniques, dans lesquelles doit être mis en œuvre l'*IAM*. Il tient compte à cet égard des intérêts de tous les Stakeholders et implique tous les autres acteurs dans la définition de manière appropriée. Les *IAM Regulators* peuvent prendre plusieurs formes et agir aussi bien au sein d'une seule organisation qu'entre plusieurs. Le *pilotage IAM* définit l'IAM Policy pour un système IAM externe ou interne à l'organisation ou pour des *services IAM*. Ce faisant, il veille également à l'orchestration, au développement stratégique continu et à la gouvernance du système IAM global. Le *législateur* définit les conditions générales juridiques dans lesquelles le système IAM global doit opérer et se développer. L'*organe de normalisation* élabore les normes et directives pour les conditions générales procédurales, organisationnelles/architecturales et techniques. Principaux Stakeholders: *Regulator*
IAM Support	L'*IAM Support* est responsable de l'ensemble des activités visant à repérer et résoudre les problèmes dans le système IAM. Principaux Stakeholders: *prestataires de service*

Relying Party	Le *Relying Party* représente les intérêts de la *ressource* dans le système IAM. Il utilise les *services IAM* et traite les informations des *prestataires de services IAM* pour protéger leurs *ressources*. *C*oncernant les *droits d'accès* et les *règles d'entrée*, il stipule, pour la *période de définition,* quelles *E-Identities* sont autorisées à accéder à leurs *ressources* et dans quelles conditions. Il a besoin, pour vérifier l'*autorisation* d'un accès aux ressources pour la *période d'exécution,* d'informations plus détaillées (propriétés pertinentes pour l'autorisation) concernant un *sujet,* son *E-Identity* et le contexte de l'*accès* (lieu, moment, *niveau de confiance* etc.). Principaux Stakeholders: *fournisseur de prestations*

Sujet	Une *personne physique*, une o*rganisation* (*personne morale)*, un *service* ou une *chose*, qui accède ou souhaite accéder à une *ressource*. Un *sujet* est représenté par une ou plusieurs *E-Identities*. Principaux Stakeholders: *bénéficiaire de prestations*

Les acteurs peuvent se répéter dans différentes unités d'organisation. Il en résulte une coopération technique à différents niveaux et dans différents contextes.

La Figure 4 présente, à l'exemple simple d'une *Identity Federation* composée d'un *RP* et d'un *prestataire de services IAM,* la coopération. Elle expose une situation. Un *sujet* souhaite se procurer des prestations techniques auprès de l'organisation 1 et est authentifié par l'organisation 2. Les organisations ont chacune une *direction* et un *Regulator*. A l'intérieur du système IAM global, on trouve une *direction* et un *Regulator* (organisation 3), qui définissent le système IAM global. L'Association eCH est un exemple d'organe de normalisation.

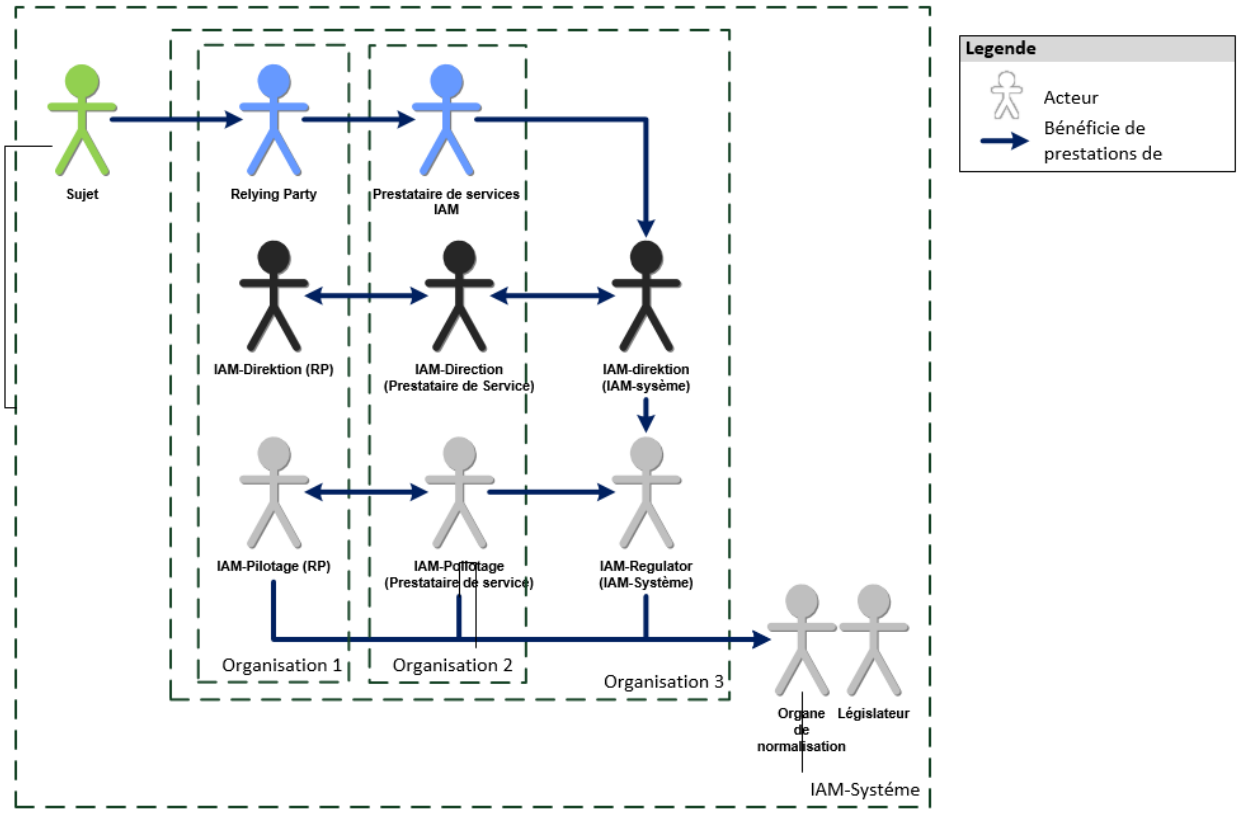


Figure 4 Coopération entre les acteurs dans un *système IAM fédéré*

4 Exigences

Les principes et exigences décrits et définis dans ce chapitre définissent et structurent les processus modélisés au chapitre 6 et doivent être appliqués ou remplis pour permettre la mise en place d'un *système IAM fédéré* interopérable et efficace.

Les principes et exigences suivants doivent être considérés comme une base. Ils peuvent être utilisés comme fondement d'un système IAM à mettre en œuvre et être complétés ou adaptés en fonction du contexte et du champ d'application.

Les principes et exigences peuvent être répartis en quatre groupes typologiques distincts:

- B… Business (exigences commerciales),
- D… Data (informations et données),
- A… Application (application),
- T… Technology (technologie).

4.1 Principes de base d'un système IAM fédéré

Les principes de base décrivent les principes architecturaux généraux pour la conception d'un système IAM fédéré. Ils prescrivent les garde-fous pour la réalisation d'un *système IAM fédératif*.

Désignation	Type	Description	Justification
Principe-1	A/B	Les informations et les données DOIVENT être non pas répliquées mais fédérées, ce qui signifie que l'accès aux données de la source d'autorité se fait directement dans le cas de l'*authentification* et de l'*autorisation* pour la *période d'exécution*, sans qu'il ne faille présenter une copie de ces données.	Actualité et cohérence des données, coûts (simplification des processus), moins sensible aux erreurs
Principe-2	A/B	Dans la mesure où le *niveau de confiance* le permet, les *E-Identities* et les *confirmations d'authentification* et *d'attribut* existantes DEVRAIENT être reprises par d'autres instances (fédération).	Réutilisable donc plus efficace
Principe-3	A	Concernant l'*authentification* et l'*entrée,* les *Relying Parties* DEVRAIENT utiliser des services (IAM) qui ne lui sont pas associés.	Coûts, modularité, extensibilité (nouvelles technologies)
Principe-4	A	L'*autorisation* d'*accès* à une *ressource* digne d'être protégée DOIT imposer que le *sujet* accédant *s'authentifie* préalablement.	Constatation de l'identité du *sujet* comme base d'une autorisation
Principe-5	A/D	Concernant l'autorisation, les procédés principalement basés sur des règles, s'appuyant sur les *attributs* (*ABAC*), DEVRAIENT être utilisés plutôt que des	Les procédés basés sur la requête nécessitent que l'identité soit préalablement

Désignation	Type	Description	Justification
		procédés basés sur une requête (approbation des rôles, *RBAC*).	transférée au gestionnaire d'autorisation
Principe-5.1	A	L'*entrée* DOIT être accordée exclusivement sur la base des *attributs* indiqués.	Indépendance de la décision relative à l'entrée dans les données de la ressource, modularité
Principe-6	B	L'efficacité inter-organisations de l'IAM DOIT s'appuyer sur une confiance mutuelle spécifique entre les partenaires.	Pas de fédération possible sans confiance
Principe-7	A/D	Dans la mesure où cela ne s'impose pas d'un point de vue technique, aucune information sur un *sujet* accédant ne DEVRAIENT être transmise à la *ressource*, hormis celles qui sont nécessaires à la décision relative à l'accès.	Principe du Need-to-Know, protection de la vie privée
Principe-8	B	Les conditions-cadre légales (de la protection des données en particulier) DOIVENT être garanties à tout moment. Le respect des règles organisationnelles/architecturales, techniques et relatives à la sécurité et les conditions-cadre techniques (dans la mesure où elles ne sont pas stipulées dans les conditions-cadre légales) DEVRAIT être garanti à tout moment.	Compliance, Interopérabilité
Principe-9	B	L'IAM DEVRAIT être géré et exploité de manière aussi économique, efficace et peu coûteuse que possible.	Coûts
Principe-10	B	Dans un souci de garantir une coopération efficace, l'*IAM* DEVRAIT être basé sur une *architecture IAM* offrant une interopérabilité au niveau international. [4]	Interopérabilité

4.2 Exigences imposées au système IAM fédéré

Cette section décrit les exigences génériques de tous les Stakeholders à un système *IAM fédéré* dans la cyberadministration suisse.

Désignation	Type	Description	Justification / principe
IAM-1	T/A	L'IAM DEVRAIT être basé sur une *architecture IAM* offrant une interopérabilité au niveau international. [4]	Principe-1 Principe-10

Désignation	Type	Description	Justification / principe
IAM-1.1	T/A	L'IAM DOIT pouvoir être intégré de manière simple à d'autres *IAM*[3]. Son intégration au niveau international DEVRAIT se faire sans difficulté.	Principe-10
IAM-1.2	T/A	L'IAM DOIT être capable d'intégrer facilement les solutions IAM existantes.	Principe-10
IAM-2	A/D	L'*authentification* et l'*autorisation* pour l'entrée DEVRAIENT *reposer* sur des *attributs* et des *moyens d'authentification* **standardisés**.	Principe-3 Principe-5.1 Principe-9 Principe-10
IAM-3	T/A	Les systèmes IAM DOIVENT présenter une structure modulaire et DEVRAIENT présenter une structure échelonnable.	Réutilisabilité, Maintenabilité Principe-9 Principe-10
IAM-4	A	Les services techniques DOIVENT coopérer via des interfaces standardisées, qui utilisent des normes ouvertes en fonction de leur spécification (par exemple SAML, OIDC).	Principe-10
IAM-5	T	Les procédés d'authentification et d'autorisation, de différentes forces et dont la nécessité dépend des besoins en protection, PEUVENT être réalisés sur la même structure IAM.	Réutilisabilité Principe-9 Principe-10
IAM-6	D	Le nombre d'*E-Identities*, *moyens d'authentification* et *attributs* DEVRAIT être réduit au minimum et, là où faire se peut, consolidé.	Convivialité Principe-9
IAM-7	A	Le transport de données DOIT être sécurisé entre les *prestataires de services IAM* et les *RP* ainsi que les *Client Platforms* au niveau du protocole (avec TLS par exemple).	Sécurité, protection de la vie privée Principe-8
IAM-8	A	Les services techniques, qui produisent ou consomment des *confirmations d'authentification et d'attribut*, DOIVENT synchroniser leurs horloges avec un serveur temporel agréé.	Sécurité, solidité Principe-10
IAM-9	B/A	L'authenticité et l'intégrité des *confirmations d'authentification et d'attribut* produites par les *services IAM* DOIVENT pouvoir être contrôlées (à l'aide d'une signature ou par des questions par exemple).	Sécurité, Trust Principe-6

[3] Les *E-Identities* peuvent être utilisées au-delà des limites des domaines grâce à l'intégration de systèmes IAM. Une telle intégration permet aux *sujets* d'un *domaine* d'accéder aux *ressources* d'un autre *domaine*, sans que les informations relatives à l'identité (*E-Identities* et *attributs* correspondants) ne doivent être gérées ou répliquées à plusieurs reprises; en d'autres termes les *E-Identities* doivent être fédérées.

Désignation	Type	Description	Justification / principe
IAM-10	A/B	La possibilité de suivre et de prouver quel *sujet* a accédé à quelle *ressource* et quand DOIT être garantie pendant une période raisonnable.	Traçabilité, Principe-8
IAM-11	B/A/T	L'exigence de sécurité, imposant que les *confirmations d'authentification et d'attribut* puissent être lues uniquement par les instances autorisées, DOIT donc être garantie.	Protection de la vie privée, Principe-8

4.3 Exigences du Stakeholder

Les exigences du Stakeholder aux différents acteurs dans un système IAM sont représentées dans le Tableau 3 sous forme de vue d'ensemble. Elles seront explicitées une par une dans les pages qui suivent et référencent aussi bien les principes de base (chap. 4.1) et les exigences (chap. 4.2) d'un système IAM fédéré que les exigences d'autres Stakeholders.

Rôles **Stakeholder**	**Sujet**	**Relying Party**	**Prestataire de services IAM**	**Direction IAM**	**IAM-Support**	**IAM Regulator**
Bénéficiaires de prestations	X	X	X		X	X
Fournisseurs de prestations	X		X	X	X	X
Prestataires de service	X		X	X		X
Direction		X	X	X	X	X
Regulator				X		X

Tableau 3 Exigences des Stakeholders aux acteurs

4.3.1 Bénéficiaire de prestations (LB)

Bénéficiaire de prestations	Le *bénéficiaire de prestations* souhaite à tout moment obtenir de manière simple et économique une prestation technique en ligne[4]. Il demande à être soutenu en cas de problèmes (usurpation d'identité par exemple) et attend que l'on se conforme aux règles légales.

[4] Il peut s'agir dans le cas de la prestation mentionnée, de la commande d'une licence radio ou d'une carte de stationnement par exemple, et pas d'une prestation IAM par un prestataire de services IAM.

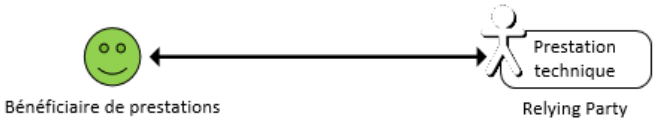


Figure 5: Point de vue du bénéficiaire de prestations

La Figure 5 présente le point de vue du *bénéficiaire de prestations* sur le système IAM global. Le *bénéficiaire de prestations* souhaite en premier lieu obtenir une prestation technique d'une *Relying Party*. Pour lui, le système IAM utilisé est secondaire, car seulement un moyen de parvenir à ses fins.

4.3.1.1 Exigences du Stakeholder: bénéficiaire de prestations

Les exigences du *bénéficiaire de prestations (BP)* sont posées par les *personnes physiques*, *organisations*, *services* ou *choses*, qui veulent accéder aux informations et services des *ressources*.

Désignation	Type	Description	Justification	Référence
BP-1	A/D	Lorsque le *sujet* accède à une *ressource* digne d'être protégée, le *sujet* DOIT s'authentifier.	*Authentification* comme base de l'*autorisation*, protection des données	**Principe-4**
BP-1.1	B/A/T	Le *sujet* DOIT s'authentifier au minimum avec le *niveau de confiance* exigé. Il PEUT s'authentifier avec un *niveau de confiance* plus élevé.	Coûts, convivialité, protection de la vie privée	**Principe-7, Principe-5**
BP-2	D	Un *identifiant* sans ambigüité par rapport à la *ressource* ne DOIT être utilisé par le *sujet* que lorsque l'utilisation de la *ressource* l'exige.	Protection de la vie privée	**Principe-7**
BP-2.1	D	Un *identifiant* aléatoire (Transient ID par exemple) par rapport à la *ressource* DEVRAIT être employé par le *sujet* lors de l'utilisation.	Protection de la vie privée (Unlinkability)	**Principe-7**
BP-3	D	Seuls les *attributs* du *sujet*, qui sont nécessaires à l'*autorisation* de la *ressource,* DOIVENT être transmis lors de l'*authentification*.	Principe du Need-to-Know, protection de la vie privée	**Principe-7**
BP-3.1	D	D'autres *attributs* PEUVENT être transmis par le *sujet* à la *ressource*.	Protection de la vie privée	**Principe-7**
BP-4	B/A	Les *prestataires de services IAM* (*IdP*, *AP*), qui gèrent les *E-Identities*	Autodétermination, liberté de choix	**Principe-2**

Désignation	Type	Description	Justification	Référence
		et les *attributs*, PEUVENT être choisis par le *sujet*.		
BP-5	D	Le nombre d'*E-Identities* nécessaires, que doit avoir le *sujet*, DEVRAIT être réduit au minimum.	Coûts, convivialité, couverture du contexte	**IAM-6**
BP-6	B	Le système IAM DEVRAIT offrir la possibilité au *sujet* de déterminer lui-même le nombre de *moyens d'authentification* et d'*attributs* de différentes qualités.	Autodétermination, liberté de choix	
BP-7	B	Le système IAM DEVRAIT offrir la possibilité au *sujet* de déterminer lui-même le *moyen d'authentification* (au cours de l'*authentification*), qui remplit l'exigence de qualité minimale requise.	Autodétermination, liberté de choix	**Principe-2**
BP-8	B	L'obtention d'*E-Identities* et de *moyens d'authentification* DEVRAIT être simple et peu coûteux.	Coûts	**Principe-9**
BP-9	A	L'utilisation d'*E-Identities* et de *moyens d'authentification* DEVRAIT être simple et sans difficulté.	Convivialité	
BP-10	B	Un autre *sujet* DEVRAIT être capable, d'agir en qualité de suppléant selon le contexte et pour une durée déterminée.	Délégation d'autorisations	
BP-11	B/A	Le *sujet* DOIT pouvoir consentir à la transmission d'*attributs*, sauf lorsque le droit de transmission est ancré dans la législation ou réglé d'une autre manière.	Protection de la vie privée	**Principe-8**
BP-11.1		Le sujet DOIT avoir à tout moment la possibilité de revenir sur son consentement	Protection de la vie privée	**Principe-8**
BP-12	B/A	Le *sujet* DOIT être soutenu concernant la prévention et au rétablissement suite à une utilisation abusive d'une E-Identity. [4]	Convivialité, sécurité	**Dir-3**
BP-13	B/A/T	*Les prestataires de services IAM DOIVENT* faire tout ce qui est raisonnablement faisable afin d'empêcher que l'*E-Identity* du *sujet* ne soit utilisée de manière abusive. [4]	Protection de la vie privée, sécurité	**FP-10, Dir-3**
BP-14	A	L'*IAM Support* DOIT soutenir le *sujet* dans la résolution des problèmes, qui	Convivialité	**Dir-6**

Désignation	Type	Description	Justification	Référence
		empêchent la réussite de l'entrée/accès à la *ressource*.		
BP-15	A	Les *attributs* validés par le *sujet* DEVRAIENT pouvoir être lus uniquement par les instances autorisées.	Protection de la vie privée	**IAM-11**
BP-16	B	L'utilisation des IAM-services pour la période *d'exécution* DOIT être possible à tout moment.[5]	Disponibilité	
BP-17	D	Lorsque la *ressource*, à laquelle le *sujet* souhaite accéder, contient des données sensibles en rapport avec le sujet, le *RP* DOIT veiller à ce que seuls les *sujets* autorisés bénéficient de l'*accès*.	Protection de la vie privée, protection des données	**Principe-4**

4.3.2 Fournisseurs de prestations (LE)

Fournisseur de prestations	Le *fournisseur de prestations* souhaite proposer des prestations techniques en ligne. Ceci devrait se faire de façon économique, stable, simple et conforme aux règles légales et être utilisés par autant d'utilisateurs que possible. Il souhaite transmettre l'*accès* et la protection des *ressources* au *prestataire de services IAM* en fonction de ses besoins (propension au risque, rentabilité par exemple).

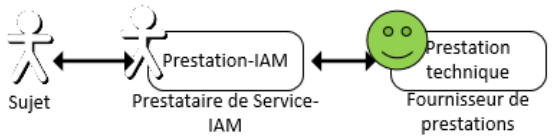


Figure 6 Point de vue du fournisseur de prestations

La Figure 6 présente le point de vue du *Fournisseurs de prestations* sur le système IAM global. Le *fournisseur de prestations* souhaite mettre sa prestation technique à la disposition du *sujet*. La plupart du temps, il ne souhaite pas fournir lui-même les prestations IAM nécessaires à cela (plusieurs *services IAM*), mais les confie à un *prestataire de services IAM* (outsourcing).

4.3.2.1 Exigences du Stakeholder: fournisseur de prestations

Cette section décrit les exigences imposées par les *fournisseurs de prestations (FP)*.

[5] La ressource devrait être utilisable à tout moment.

Désignation	Type	Description	Justification	Référence
FP-1	B/A/T	L'*entrée/accès* non autorisé de *ressources* DOIT être empêché.	Sécurité	
FP-2	A	L'*accès* aux ressources dignes de protection DOIT être limité aux *sujets* autorisés.	Sécurité (Access Control)	**Principe-4**
FP-2.1	A	Dans l'éventualité où le *sujet* ne dispose d'aucun *droit* concernant la *ressource* digne d'être protégée et sollicitée, il DOIT rejeter la sollicitation de l'*E-Ressource* et/ou le rediriger en conséquence.	Sécurité, convivialité	
FP-3	B/A	Les efforts mis en œuvre pour gérer les *E-ressources* DEVRAIENT être réduits au minimum.	Coûts	**Principe-9**
FP-4	B/A	Les efforts mis en œuvre pour gérer les *autorisations* (*règles d'entrée* et *droits d'accès*) DEVRAIENT être minimaux.	Coûts	**Principe-9**
FP-5	D	Le nombre d'*E-Identities* et d'*attributs* soutenus DOIT être réduit au minimum et DEVRAIT, dans la mesure du possible, être consolidé.	Coûts	**Principe-9, IAM-6, BP-5**
FP-6	B	Les *E-Identities* et *attributs* DOIVENT être mis à jour rapidement en cas de modifications.	Actualité	
FP-7	A	*Les confirmations d'authentification* et *d'attribut* PEUVENT être délivrées par les *prestataires de services IAM* dans une qualité différente. [4] La qualité DEVRAIT être une partie intégrante de la confirmation *confirmations* ou *d'authentification*	Interopérabilité	**Principe-2**
FP-8	B	*Des attributs* identifiant le *sujet* DEVRAIENT être présents dans la *confirmation d'authentification* et/ou *d'attribut* pour les *sujets*.	Reconnaissance du sujet	
FP-9	B	Le *sujet* et les *prestataires de services IAM* DOIVENT signaler tout soupçon d'utilisation abusive d'une E-Identity. [4]	Sécurité	
FP-10	B/A/T	Les *prestataires de services IAM DOIVENT* faire tout ce qui est raisonnablement faisable afin d'empêcher	Protection de la vie privée, sécurité	**BP-13 Dir-3**

Désignation	Type	Description	Justification	Référence
		que l'utilisation abusive de l'*E-Identity* du *sujet*. [4]		
FP-11	B/A	Dans un modèle de fédération avec un *Broker* central, le *fournisseur de prestations* DEVRAIT déléguer autant de responsabilités d'exploitation que possible au *Broker*.	Coûts, intégration/configuration simple, Interopérabilité	**Principe-9**

4.3.3 Prestataire de service

Prestataire de service	Le *prestataire de service* souhaite que les prestations IAM qu'il propose soient utilisées par autant d'utilisateurs que possible. En outre, il s'efforce de regrouper des services aussi complémentaires que possible afin de préserver toute l'efficacité et le caractère économique du système IAM.

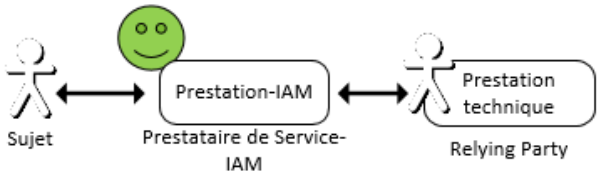


Figure 7 Point de vue du prestataire de services

Figure 7 présente le point de vue du *prestataire de services* sur le système IAM global. Le *prestataire de service* met sa prestation IAM à disposition du *Relying Party* et du sujet. Le *sujet* peut utiliser la prestation technique du *Relying Party* à l'aide de cette prestation IAM.

4.3.3.1 Exigences du prestataire de service

Cette section décrit les exigences du prestataire de service.

Désignation	Type	Description	Justification	Référence
Service-1	B/A	Les efforts mis en œuvre concernant l'administration des *E-Identities* (*moyens d'authentification* et *attributs*) DEVRAIENT être minimaux par rapport à la qualité visée.	Coûts	**Principe-9, BP-8**
Service-2	D	Le rapport entre l'*E-Identity* et les *moyens d'authentification* correspondants DOIT être garanti à tout moment.	Traçabilité	**IAM-10**
Service-3	B	La *direction IAM* DOIT garantir la stabilité des aspects procéduraux, organi-	Coûts, protection des investissements	**Principe-9**

Désignation	Type	Description	Justification	Référence
		sationnels/architecturaux et techniques du système IAM et la poursuite du développement.		

4.3.4 Stakeholder Direction

Direction	La *direction* souhaite un système IAM stable et performant, qui conviennent à tous les Stakeholders. Elle dirige les *prestataires de services IAM* et les *Relying Parties* impliqués et garantit le fonctionnement fiable du système IAM.

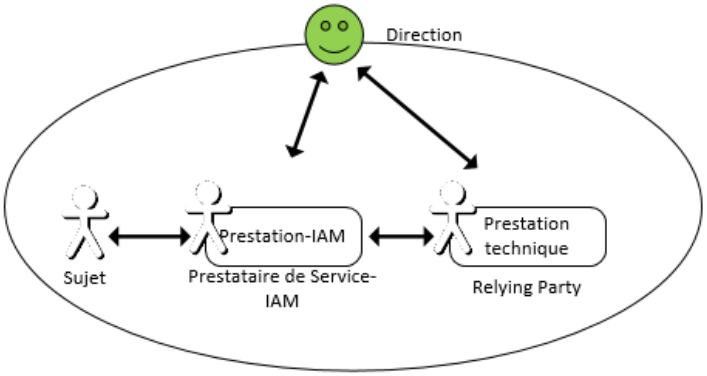


Figure 8 Point de vue de la direction du système global IAM

La Figure 8 présente le point de vue de la *Direction* du système IAM global. La *direction* souhaite diriger efficacement le système IAM et les *Relying Parties* et *prestataires de services IAM* impliqués afin de faciliter l'implémentation et de garantir le fonctionnement fiable. La *Direction* coordonne à cet égard les exigences de tous les Stakeholders dans le système IAM, celles du *régulateur* et du *bénéficiaire de prestation*.

4.3.4.1 Exigences du Stakeholder: Direction

Cette section décrit les exigences du Stakeholder *Direction*.

Désignation	Type	Description	Justification	Référence
Dir-1	B/A	Le *prestataire de services IAM* et les *Relying Parties* DEVRAIENT s'entendre sur un nombre de *moyens d'authentification* et d'*attributs*.	Interopérabilité, convivialité, «dirigeabilité»	**IAM-2, IAM-6, IAM-7**
Dir-2	T	Le *prestataire de services IAM* et les *Relying Parties* DOIVENT utiliser des interfaces standardisées.	Interopérabilité	**IAM-4**

Désignation	Type	Description	Justification	Référence
Dir-3	B/A	Les différents *prestataires de services IAM* et *Relying Parties* DOIVENT collaborer afin de soutenir le *sujet* dans la prévention et le rétablissement suite à l'utilisation abusive d'une E-Identity.	Convivialité, sécurité	**BP-12, BP-13, FP-10**
Dir-4	B/D	Les différents *prestataires de services IAM* et les *Relying Parties* DOIVENT coopérer afin qu'il soit possible à tout moment de suivre quel *sujet* a accédé à quelle *ressource* et quand.	Traçabilité	**IAM-10**
Dir-5	B	L'*IAM Regulator* DOIT définir les conditions générales légales, procédurales, organisationnelles/architecturales et techniques requises pour le système IAM concerné.	Conformité au droit, sécurité, solidité	**Principe-8 Reg-1**
Dir-5.1	B	Les différents *prestataires de services IAM* et les *Relying Parties* DEVRAIENT respecter les conditions générales définies par l'*IAM Regulator*.	Conformité au droit, Sécurité, solidité	**Principe-8**
Dir-6	A	L'*IAM Support* DOIT soutenir le *sujet* de manière efficace, conviviale, économique et intelligible dans la résolution des problèmes qui empêchent l''entrée/l'accès à la *ressource*.	Convivialité, coûts	**BP-14**

4.3.5 Regulator

Regulator	Le *Regulator* souhaite garantir l'interopérabilité (dans le cas de sous-systèmes dirigés de manière autonome en particulier), la solidité et la sécurité du système IAM global.

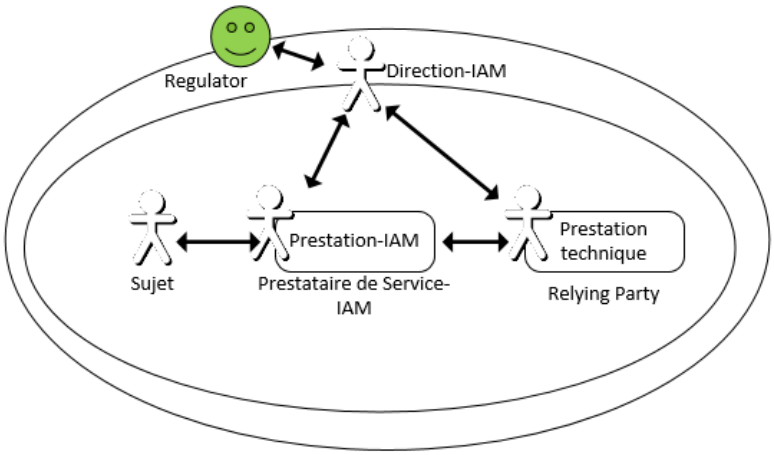


Figure 9 Point de vue du Regulator

La Figure 9 présente le point de vue du *Regulator*. Le *Regulator* souhaite, en réunissant les conditions générales correspondantes (lois, normes, stratégies, etc.), promouvoir l'utilisation de systèmes IAM fédérés dans le contexte inter-organisations et, dans le même temps, obtenir une qualité élevée d'aspects non fonctionnels, comme l'interopérabilité, la fiabilité et la sécurité par exemple.

4.3.5.1 Exigences du Stakeholder: Regulator

Cette section décrit les exigences du Stakeholder *Regulator*.

Désignation	Type	Description	Justification	Référence
Reg-1	B	Les différents *prestataires de services IAM* et *Relying Parties* DOIVENT respecter les conditions générales légales, Les différents *prestataires de services IAM* et *Relying Parties* DEVRAIENT (dans la mesure où elles ne sont pas stipulées dans les conditions générales légales) respecter les conditions générales procédurales, organisationnelles/architecturales et techniques définies.	Compliance, lois applicables sur la protection des données et règles cantonales sur la protection des données	**Principe-8** **Dir-5**
Reg-2	B	Le respect des conditions générales légales, procédurales, organisationnelles/architecturales et techniques définies DOIT pouvoir être attesté par les justificatifs correspondantes.	Compliance	**Principe-8**
Reg-3	B	En cas de non-respect, la *direction IAM* DOIT demander et faire valider une dérogation motivée.	Gestion des risques	**Principe-8**

5 Architecture d'information

Le modèle ci-dessous présente les termes-clés de l'*IAM*, ainsi que leurs relations dans une vue d'ensemble représentée sous forme de diagramme de classes UML. Les éléments du modèle d'information *IAM* étant utilisés dans de nombreux endroits (pas uniquement dans l'*IAM*), il est capital d'utiliser des termes nuancés afin que la syntaxe et la sémantique puissent être définies de manière précise et claire pour tous les intéressés. La Figure 10 présente le modèle d'information relative à l'IAM inter-organisations.

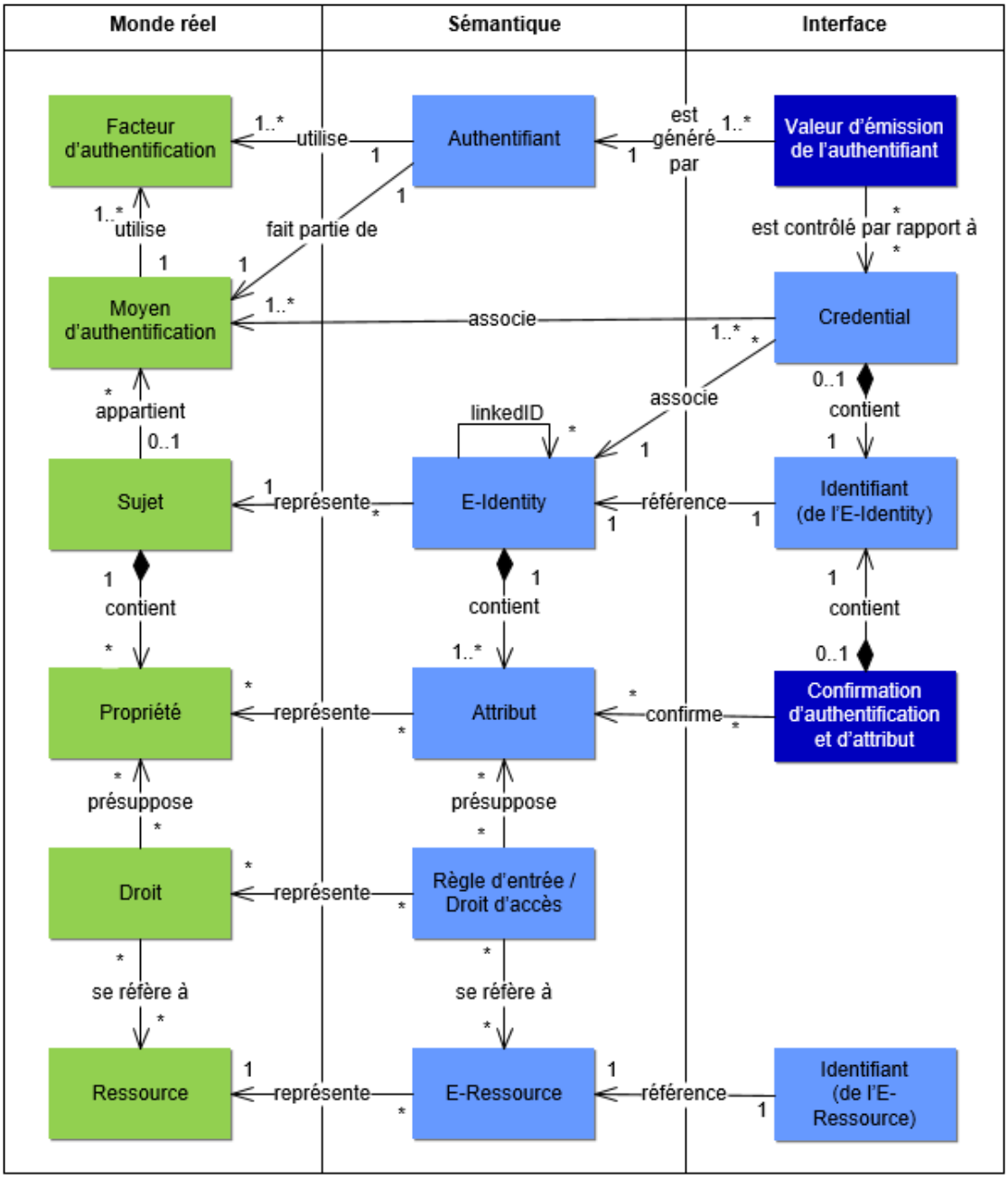


Figure 10 Modèle d'information

Il est courant d'utiliser les mêmes marqueurs entre le domaine spécialisé et les systèmes d'information pour les éléments du monde réel. Puisque les différences entre l'aspect sémantique (les systèmes d'information concernés) et le monde réel sont fondamentales, on utilisera ici différents marqueurs pour les différents éléments. Le modèle d'information de la Figure 10 indique à gauche (en vert) les éléments du monde réel, au centre le modèle sémantique (des systèmes d'information), et à droite, les objets de l'interface utilisés pour l'échange d'informations entre les différents systèmes d'informations. Les objets, qui sont créés pendant la *période de définition*, sont représentés en bleu clair, les objets pendant la *période d'exécution* en bleu foncé, conformément au code de couleurs exposé dans le Tableau 1.

Le modèle sémantique au centre ne fait aucun commentaire concernant la répartition de l'information dans les systèmes d'information.

Les objets du monde réel ainsi que leurs caractéristiques et relations dans les systèmes d'information (sémantique) sont représentés pour la *période de définition* (voir processus de la section **Fehler! Verweisquelle konnte nicht gefunden werden.** et Services IAM de la section 7.2).

Concernant la *période d'exécution* (voir les processus de la section 6.1 et les services IAM de la section 7.3), les objets d'interface sont créés sur la base des contenus du modèle sémantique et échangés entre les systèmes d'information.

Le tableau suivant décrit de manière concise[6] les éléments figurant dans la Figure 10 et leurs relations.

Monde réel	
Ressource	Service ou données, ou données auxquels un *sujet* peut accéder lorsqu'il s'est *authentifié* et que l'accès a été *autorisé*, sur la base des *attributs* requis. Ceci inclut les ressources physiques telles que bâtiments et installations, dont l'utilisation est gérée par des systèmes informatiques.
Droit	Les *droits* sont des *propriétés* spécifiques abstraites, que le *sujet* doit posséder pour pouvoir accéder à une *ressource*. Celles-ci peuvent par exemple être stipulées dans la loi ou un contrat.
Propriétés	*Les propriétés* sont des caractéristiques typiques ou un comportement caractéristique d'un *sujet*, qui sont propres au sujet dans leur ensemble.

[6] Pour des descriptions complètes avec illustrations et exemples, se reporter au document eCH-0219 [1].

Sujet

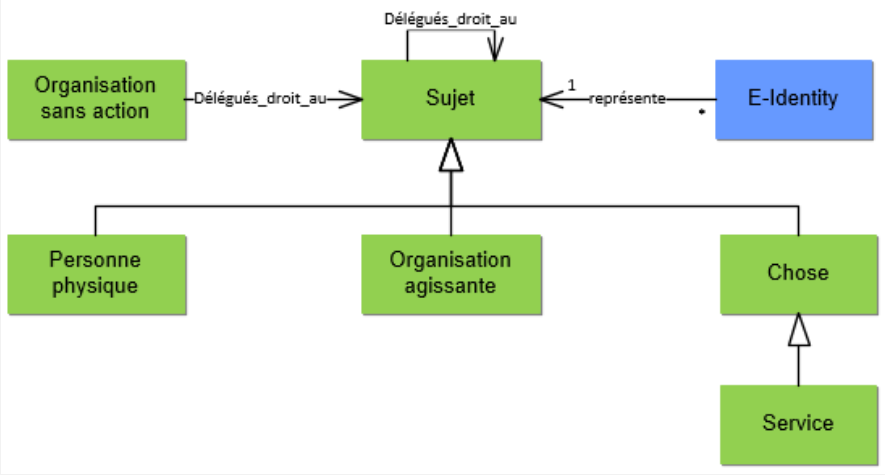


Figure 11 Définition du s*ujet*

Un *sujet* est une *personne physique*, une *organisation* agissante, un *service* ou une *chose*, qui accède ou souhaite accéder à une *ressource*.

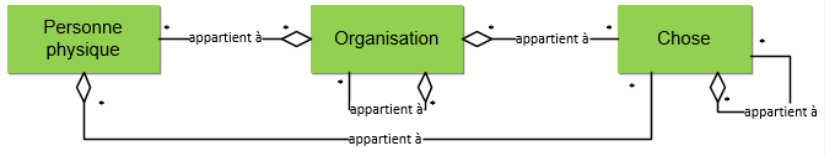
Un *sujet* est représenté par des *E-Identities* dans le monde numérique.

Un *sujet* peut déléguer des *droits* à un autre *sujet*.

Une *organisation* est un groupe de plusieurs *personnes physiques* ou *choses*. Une *organisation* peut contenir des (sous-)organisations.

On établit à cet égard une distinction entre les organisations *agissantes* et *non-agissantes*. *Les organisations agissantes* (identités des groupes par exemple) peuvent s'authentifier et se voir accorder l'*accès* aux *ressources*. Les *organisations non agissantes* (*personnes morales* par exemple) ne peuvent s'authentifier elles-mêmes, mais uniquement via le *sujet* correspondant (une *personne physique* par exemple) auquel elles délèguent leurs *droits*.

Une *personne morale* est une *organisation spéciale*, qui est reconnue par une *autorité* habilitée à reconnaître. Cette reconnaissance repose sur un contrat souscrit entre l'*autorité* habilitée à reconnaître et la *personne morale*. A une *personne morale* doit toujours être assignée au moins une *personne physique*.

	Une *chose* est une unité existante ou abstraite pouvant être identifiée sans ambigüité.  **Figure 12 Appartenance des *sujets*** Une *chose* peut en contenir d'autres et appartenir à une *organisation* ou une *personne physique*. Un *service* est une *chose* particulière, à laquelle on peut accéder via un *réseau* et dans lequel elle peut être identifiée par des moyens numériques.
Moyen d'authentification	Quelque chose qu'un *sujet* a en sa possession et dont il a le contrôle (clé cryptographique, secret ou comportement spécifique). Un *moyen d'authentification* peut utiliser un seul (*single-factor authenticité*) ou plusieurs *facteurs d'identification* (*multi-factor authenticité*) indépendants.
Facteur d'authentification	Informations et/ou processus, qui peuvent être utilisés à des fins d'*authentification* d'un *sujet*. Les *facteurs d'identification* peuvent s'appuyer sur quatre caractères distincts (basé la possession, basé sur la connaissance, inhérent ou basé sur le comportement) ou des combinaisons de ces caractères.
Sémantique	
E-Ressource	Représentation numérique d'une *ressource*. Une *E-Ressource* a un *Identifiant* (nom unique, souvent une URL/URI) pouvant être affecté à une *ressource* de manière explicite dans le cadre d'un *espace de noms*.
Règles d'entrée / droit d'accès	Les responsables des *ressources* définissent les *règles d'entrée* et les *droits d'accès* à leurs *E-ressources*. Les *règles d'entrée* et les *droits d'accès* définissent les conditions dans lesquelles un *sujet* bénéficie d'un droit d'entrée concernant une *ressource* (*autorisation grossière*) et peut y accéder (*autorisation précise*), par exemple lorsque *l'authentification* a été effectuée et que les *attributs* définis ont été validés.
Attribut	La représentation sémantique d'une *propriété* attribuée à un *sujet*, qui décrit le *sujet* de manière plus approfondie. L'*identifiant* est également un *attribut* utilisé de manière spécifique.

E-Identity	Représentation d'un *sujet*. Une *E-Identity* (*identité numérique*) comprend un *identifiant* (nom explicite), le plus souvent accompagné d'une quantité d'*attributs* supplémentaires pouvant être affectés à un *sujet* de manière explicite dans le cadre d'un *espace de noms* (et donc d'un *domaine*). Un *sujet* peut posséder plusieurs *E-Identities*.[7]
linkedID (Relation)	Dans le contexte inter-organisations, la relation *linkedID* permet de mettre en rapport les *E-Identities* de différents *domaines*. Les *E-Identities* peuvent être associées à n'importe quel graphique avec des *linkedID*. La mise en œuvre concrète d'eCH-0107 peut restreindre encore la forme (ex. arborescence au lieu du graphique) et règle l'interprétation (sémantique) du graphique en fonction de leurs compétences (voir 7.3.4 *Broker Service*).
Authentificateur	Représentation fonctionnelle du *moyen d'authentification* du monde réel. Une valeur d'émission est générée à partir d'une valeur de saisie et d'une valeur secrète avec la fonction d'un *authentifiant*.
Interface	
Confirmation d'authentification et d'attribut	Confirmation d'*authentification* réussie d'un *sujet* (*confirmation d'authentification*) ou confirmation de la valeur d'un *attribut* (*confirmation d'attribut*). Contient un *identifiant*.
Identifiant	Chaîne de caractères qui définit explicitement une *E-Identity* ou une *E-Ressource*, dans le cadre d'un *espace de noms (domaine)*.
Credential	Représente un volume de données permettant d'associer une *E-Identity* à un *moyen d'authentification* détenu & contrôlé par le sujet.
Valeur d'émission de l'authentifiant	Est générée par une fonction mathématique (*Authentificateur* ou fonction d'authentification) à partir d'une valeur secrète (clé privée par exemple), d'une ou de plusieurs valeurs d'activation facultatives (PIN ou informations biométriques par exemple), et d'une ou de plusieurs valeurs de saisie facultatives (valeurs aléatoires ou Challenges par exemple). La puissance de la valeur d'émission de l'authentifiant est fonction de celle du procédé utilisé ou de sa mise en œuvre.

Tableau 4 Description des éléments du modèle d'information

[7] Cette affirmation (dans le cadre de eCH-0107) vaut pour les systèmes inter-organisations. Il est toutefois recommandé de n'imposer aucune restriction concernant l'unicité, même au sein de l'organisation.

6 Processus

La Figure 13 représente une vue d'ensemble des processus administratifs. Elle sert à illustrer les activités nécessaires à une bonne coopération entre les différents acteurs dans un système IAM (voir définitions au chapitre 3.1) Les processus en bleu constituent les processus centraux, ceux en gris les processus de direction et de régulation.

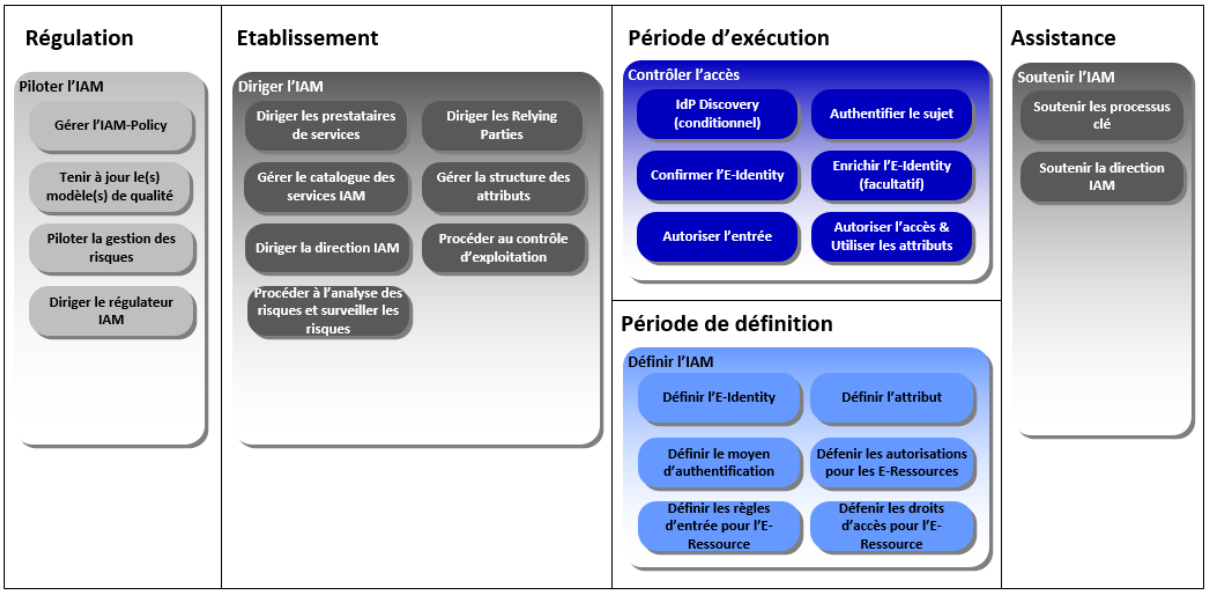


Figure 13 Cartographie des processus IAM

Les différents acteurs participent à ces processus, conformément au chapitre 3.1. Les paragraphes suivants décrivent les processus administratifs ainsi que leurs sous-processus.

Le propriétaire de processus mentionné est habituellement l'acteur ayant la responsabilité du processus. La *direction* détermine et orchestre toutefois l'affectation des processus aux acteurs sur la base de l'architecture et de la topologie.

Les activités sont en partie qualifiées de 'conditionnelles' ou 'facultatives'. 'Conditionnel' signifie que l'activité dépend du résultat d'une autre activité ou d'une activité 'facultative'. Les activités qualifiées de 'facultatives' peuvent être exécutées selon l'*architecture IAM* et/ou *IAM Policy* définie.

6.1 Contrôler l'accès (période d'exécution)

Contrôler l'accès englobe les processus de la *période d'exécution*. L'objectif de *Contrôler l'accès* est l'observation contrôlée et garantie des règles d'*accès* d'un *sujet* à une *ressource*. Lors de l'*accès* du *sujet*, celui-ci est *authentifié* puis, dans la mesure où cela est *autorisé*, l'*accès* aux *ressources* est débloqué. Dans un *système IAM fédéré*, dans lequel l'*Identity Provider* et le Relying Party sont des systèmes séparés via un *réseau*, l'*E-Identity du sujet* confirmée lors de l'*authentification* doit encore être fédérée .

Les sous-processus de *Contrôler l'accès* s'appuient les uns sur les autres dans un ordre établi (voir Figure 14).

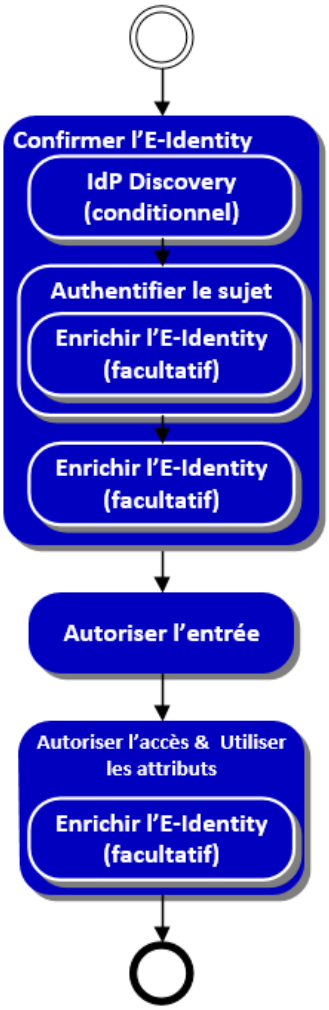


Figure 14 Diagramme du processus *Contrôler l'accès*

Dans l'intérêt d'une mise à disposition fiable d'informations, *Contrôler l'accès* garantit que seuls les *sujets* ayant le droit d'accéder à la *ressource* ont bien *accès* à celle-ci. Tous les autres se verront refuser l'*accès* aux fonctionnalités de la *ressource* ou même tout droit d'*entrée* concernant la *ressource*.

Les services IAM, qui définissent les interfaces avec les processus pendant la période d'exécution sont décrits à la section 7.3.

6.1.1 Confirmer l'E-Identity

Confirmer l'E-Identity	Générer et transmettre la confirmation de l'*E-Identity* par l'*IdP* ou le *Broker* au *RP*.

Propriétaire du processus: *RP* ou *Broker* (la *direction IAM* détermine et orchestre les compétences)

Exigences: BP-2, BP-2.1, BP-13, BP-16, FP-2, FP-8, FP-10, Dir-3

Concernant le processus *Confirmer l'E-Identity* en fonction du modèle d'Identity Federation utilisé (voir aussi le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**), un autre acteur se charge de:

Activités:

Modèle centré sur le RP ou modèles de fédération avec *Broker* (voir chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**):

- (facultatif en cas de *Broker*) Vérifier si le *RP* est en droit de demander une *confirmation d'authentification*. Si la vérification est positive, le *RP* est en droit de recevoir des *confirmations d'authentification*. Si la vérification est négative, le *RP* n'est pas autorisé et le processus est interrompu.
- (conditionnel) Dès lors que le *sujet* selon l'*IAM Policy* peut identifier pour plusieurs *IdP*, le processus *IdP Discovery* (6.1.2) est initié.
- Le processus *Authentifier le sujet* (**Fehler! Verweisquelle konnte nicht gefunden werden.**) est initié.
    - (facultatif en cas de *Broker*) Conformément aux relations *linkedID*, le processus *Authentifier le sujet* (**Fehler! Verweisquelle konnte nicht gefunden werden.**) est initié une fois (ou plusieurs fois) pour d'autres *IdP* (*Identity Mapping*).
- (facultatif) Obtient le consentement du *sujet* pour transmettre la *confirmation d'authentification* au service sollicitant. Dès lors que le *sujet* ne donne pas son consentement, le processus est interrompu.
- Génère une *confirmation d'authentification* avec estampille temporelle, signature, *identifiant* (selon exigences *RP*, *sujet* et *IAM Policy*) et chiffrage facultatif.
- (facultatif) Choisir un *AP*, qui a été relié à l'*E-Identity* au cours de la *période de définition*.
- (facultatif) Initier *Enrichir l'E-Identity* (□).
    - (facultatif en cas de *Broker*) Le *Broker* peut effectuer à plusieurs reprises *Enrichir l'E-Identity* (□) et agréger les *attributs*.
    - (facultatif en cas de *Broker*) Le *Broker* transforme les attributs selon les directives édictées par la *direction IAM*.
- (facultatif en cas de *Broker*) Le *Broker* transforme die protocoles selon les directives édictées par la *direction IAM*
- La *confirmation d'authentification* est transmise au processus *Autoriser l'entrée* (**Fehler! Verweisquelle konnte nicht gefunden werden.**).
    - (conditionnel) Dans le cas où le processus *Enrichir l'E-Identity* (□) a été initié, la *confirmation d'attribut* est transmise au processus *Autoriser l'entrée* (**Fehler! Verweisquelle konnte nicht gefunden werden.**).
- Toutes les actions et décisions prises sont enregistrées et documentées (Logging).

Modèle centré sur l'IdP/AP (voir chapitre 10.2):

- Le processus *Authentifier le sujet* (**Fehler! Verweisquelle konnte nicht gefunden werden.**) est initié.

- Génère une *confirmation d'authentification* avec estampille temporelle, signature, *identifiant* (selon les exigences *RP*, *sujet* et *IAM Policy*) et chiffrage facultatif.
- (facultatif) Choisit un *AP*, qui a été relié à l'*E-Identity* pendant la *période de définition*.
- (facultatif) Initier *Enrichir l'E-Identity* (□) le cas échéant exécuter à plusieurs reprises et agréger les *attributs*.
- (facultatif) Transforme les protocoles selon les directives édictées par la direction IAM.
- Met à disposition d'une sélection de *RP*, le *sujet* en choisit un.
- (facultatif) Obtient le consentement du *sujet* pour que la *confirmation d'authentification* et/ou *confirmation d'attribut* soient transmises au *RP* sélectionné. Dès lors que le *sujet* ne donne pas son consentement, le processus est interrompu.
- La *confirmation d'authentification* et/ou *confirmation d'attribut* sont transmises au processus *Autoriser l'entrée* (**Fehler! Verweisquelle konnte nicht gefunden werden.**).
- Toutes les actions et décisions prises sont enregistrées et documentées (Logging).

Remarques:

Dans le cas où l'*IdP* et l'*AP* tombe sur la même instance, on s'y réfère en tant qu'IdP/AP. Dans ce cas, c'est habituellement l'IdP/AP qui génère et répond aux *confirmations d'authentification et d'attribut*.

6.1.2 IdP Discovery (conditionnel)

IdP Discovery	Mise à disposition d'une sélection d'IdP pour le *sujet*.

Propriétaire du processus: *RP* ou *Broker*

Exigences: BP-1.1, BP-7, BP-16, FP-10, Dir-3

Activités:

- Met à disposition une sélection d'*IdP*, le *sujet* en choisit un.
  - (facultatif) Le choix de l'*IdP* peut être enregistré au moyen des préférences personnelles, de sorte qu'il n'est pas nécessaire de faire à nouveau un choix à chaque *accès*.
- Le *sujet* choisit un *IdP*, à partir duquel il est convaincu qu'il peut s'authentifier.
  - (facultatif) Eventuellement, proposer une aide à la décision au *sujet* ou le soutenir dans le choix de l'*IdP* et, le cas échéant, initier le processus *Soutenir les processus centraux* (0).
  - (conditionnel) Dans le cas où le *sujet* n'est pas encore enregistré, le processus *Définir l'E-Identity* (**Fehler! Verweisquelle konnte nicht gefunden werden.**) est initié.

6.1.3 Authentifier le sujet

Authentifier le sujet	Processus de vérification rapide de l'*E-Identity* supposée d'un *sujet* par un *Identity Provider*.

Propriétaire du processus: *IdP*

Exigences: BP-1, BP-9, BP-13, BP-16, FP-10, Dir-3

Activités:

- Vérifie si le service sollicitant est en droit de solliciter une *authentification*.
- Le *sujet* utilise un *moyen d'authentification* mit à sa disposition et dont il a le contrôle. (Credential Discovery)
- Le *moyen d'authentification* génère, à l'aide de l'authentifiant, une valeur d'émission à partir des saisies effectuées par le *sujet*. Le *moyen d'authentification* transmet la valeur d'émission générée à un *Verifier* à des fins de vérification.
- Le *Verifier* contrôle la valeur d'émission générée par l'authentifiant avec le *Credential* de l'*E-Identity* supposée. Si la vérification est positive, l'*authentification* a réussi et le *sujet* est authentifié. Si la vérification est négative, l'*authentification* échoue et le *sujet* n'est pas authentifié.
- (facultatif) Obtient le consentement du *sujet* (limité aux personnes physiques) pour le transfert de la *confirmation d'authentification*.
- (IdP avec AP – IdP/AP intégral) Initier (□).
- (facultatif) Etablit une connexion sûre limitée dans le temps avec la *Client Platform* du *sujet* (navigateur ou application par exemple).
- (facultatif) Peut transmettre la *confirmation d'authentification* au service sollicitant, tant qu'il y a une connexion sûre avec la *Client Platform* du *sujet* (prise en charge du Single Sign-On).

6.1.4 Enrichir l'E-Identity (facultatif)

Enrichir l'E-Identity	Enrichir les *attributs* concernant l'*E-Identity* correspondante.

Propriétaire du processus: AP

Exigences: BP-11, BP-13, BP-15, BP-16, FP-8, FP-10, Dir-3

Activités:

- L'*AP* vérifie si le service sollicitant est en droit de demander une *confirmation d'attribut*. Si la vérification est positive, le service sollicitant est en droit de recevoir une *confirmation d'attribut*. Si la vérification est négative, les *valeurs d'attribut* ne sont pas transmises et/ou un message d'erreur/exception est transmis.
- L'*AP* traite les *attributs* correspondants. Les *valeurs d'attribut* calculées et déduites des *attributs* (over18 par exemple) peuvent être générées.
- (conditionnel) dans le cas de valeurs multiples d'*attributs, le sujet* choisit une *valeur d'attribut* correspondante.

- (conditionnel) L'*AP* obtient le consentement du *sujet* concernant la transmission de la *confirmation d'attribut* au service sollicitant. Dès lors que le *sujet* y consent, la *confirmation d'attribut* est transmise. Si le *sujet* n'y consent pas, les *valeurs d'attribut* ne sont pas transmises et/ou un message d'erreur/exception est transmis.
- L'*AP* génère une *confirmation d'attribut* avec une estampille temporelle, une signature, un *identifiant* (selon les exigences service sollicitant, *sujet* et *IAM Policy*) et chiffrage facultatif.
- L'*AP* confirme, par voie électronique, avec la qualité correspondante (voir par exemple le modèle de qualité pour la confirmation d'attribut eCH-0171 [5]) qu'un *attribut* particulier est ou non affecté à un *sujet*.
- (facultatif) L'*AP* peut chiffrer la *confirmation d'attribut* pour le service appelant (ou le destinataire final).
- L'*AP* transmet la *confirmation d'attribut* au service sollicitant.
- Toutes les actions et décisions prises sont enregistrées et documentées (logging).
- **Remarques:**

L'*AP* peut être une partie intégrante d'un *IdP*. On parle dans ce cas d'un IdP/AP.

6.1.5 Autoriser l'entrée

Autoriser l'entrée	*Autorisation grossière* au moyen des r*ègles d'entrée*.

Propriétaire du processus: Broker ou RP

Exigences: BP-13, BP-16, FP-1, FP-10, Dir-3

Concernant le processus *Autoriser l'entrée,* en fonction du modèle d'Identity Federation utilisé (voir aussi le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**), un autre acteur se charge de.

Activités:

- La condition préalable à toute *autorisation grossière* est l'*authentification* réussie d'un *sujet*.
- Détermine les *règles d'entrée* pour bénéficier du droit d'*entrée* concernant l'*E-Ressource.*
- Vérifie si l'*entrée* est autorisée pour le *sujet* au moyen de l'*authentification* demandée et des *attributs* exigés, dans la qualité souhaitée. Si la vérification est positive, l'*entrée* est autorisée. Si la vérification est négative, le *sujet* se voit refuser l'entrée.
- Toutes les actions et décisions prises sont enregistrées et documentées (Logging).
- Transmet les *confirmations d'authentification* et les *confirmations d'attribut* et initie le procès *Autoriser l'accès et utiliser les attributs* (6.1.6).

6.1.6 Autoriser l'accès et utiliser les attributs

Autoriser l'accès et divulguer les attributs	Vérifier l'*autorisation d'accès* d'une *E-Identity* ayant reçu une *autorisation grossière* à une *E-Ressource* et accorder l'*accès* à une E-*Ressource* pour la *période d'exécution*. Divulguer les *attributs* du *sujet*.

Propriétaire du processus: RP

Exigences: BP-3, BP-3.1, BP-16, FP-1, FP-2, FP-2.1, FP-8

Activités:

- La condition préalable à tout *accès* est une a*utorisation grossière* accordée.
- Le *RP* vérifie l'actualité et l'authenticité de la *confirmation d'authentification*. Si la vérification est positive, l'*authentification* est réussie et le *sujet* est authentifié. Si la vérification échoue, le *sujet* n'est pas authentifié et l'*accès* est refusé.
- Le *RP* vérifie l'actualité et l'authenticité de la *confirmation d'attribut* reçue. Si la vérification est positive, les *valeurs d'attribut* sont valides et à jour. Si la vérification échoue, il revient au *RP* de réagir en conséquence.
- Le *RP* détermine les *droits d'accès* pour l'*accès* à l'*E-Ressource*. On en déduit les *valeurs d'attribut* nécessaires concernant l'*E-Identity*.
- Le *RP* vérifie qu'il y a bien les *valeurs d'attribut* nécessaires (également pour remplir sa fonction technique).
    - (conditionnel) Le propriétaire du processus choisit un *AP*, qui a été mis en relation avec l'*E-Identity* lors de la *période de définition*.
    - (conditionnel) Initier le sous-processus *Enrichir l'E-Identity* (□).
- Si les *valeurs d'attribut* nécessaires sont bien présentes, le *RP* autorise l'*accès*. Le *sujet* accède ensuite à la *ressource*. Dès lors que les *valeurs d'attribut* nécessaires ne sont pas présentes, le *sujet* se voit refuser l'accès et reçoit un message d'erreur correspondant.
- Génère un Security Token pour le *sujet* autorisé avec les *attributs* confirmés et pertinents dans le contexte de l'accès.
- Limite la durée de vie du Security Token.
- En fonction du *niveau de confiance* exigée, le *RP* doit faire à nouveau authentifier le *sujet* par l'*IdP* (re-authentification) au bout d'une durée déterminée (quelles que soient ses propres directives).
- (facultatif) Collabore avec la gestion des licences pour refuser l'*accès* par exemple, lorsque le nombre maximal d'utilisateurs simultanés est atteint.
- Toutes les actions et décisions prises sont enregistrées et documentées (Logging).

6.2 Définir l'IAM (période de définition)

Au cours de la *période de définition,* toutes les conditions nécessaires sont réunies pour permettre de déterminer, lors de la *période d'exécution,* si un *sujet* est autorisé à accéder à une *ressource* digne d'être protégée. La *période de définition* doit avoir lieu avant que le *sujet* utilise la *ressource*. La mise en œuvre de *Définir l'IAM* a une incidence très directe sur la qualité du *contrôle de l'accès*.

Définir l'IAM se compose de deux sous-processus distincts pouvant se dérouler indépendamment l'un de l'autre (voir Figure 15).

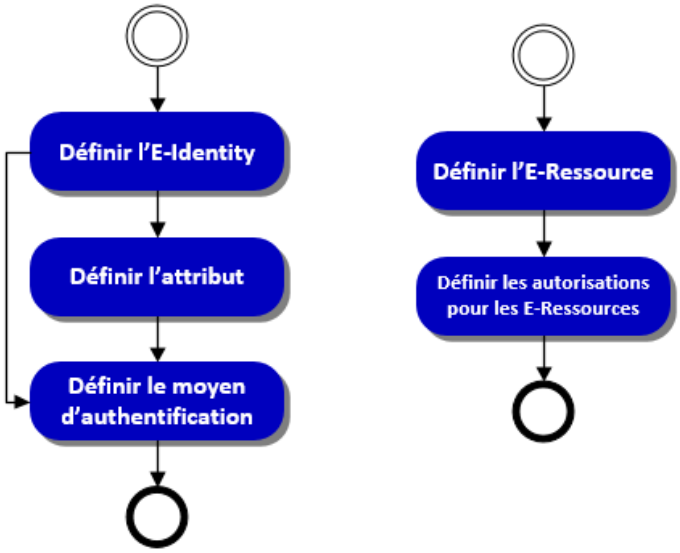


Figure 15 Diagramme du processus *Définir l'IAM* (à gauche: définir une E-Identity; à droite: définir une E-Ressource)

Les *services IAM*, qui définissent les interfaces avec les processus de la *période de définition*, sont décrits de manière plus approfondie à la section 7.2.

6.2.1 Définir l'E-Identity

Définir l'E-Identity	Comprend l'émission, la mise à jour et la gestion des *E-Identities* et de leurs relations et garantie de la qualité et de l'actualité des *E-Identities*.

Propriétaire du processus: *RA*

Exigences: BP-4, BP-5, BP-8, BP-9, BP-10, FP-5, FP-6, Service-1

Activités:

- (facultatif) Le *sujet* sélectionne choisit la *RA* parmi la quantité définie par la *direction IAM* (6.3.1 Diriger les prestataires de service).
- (facultatif) Le *sujet* est identifié selon le *niveau de confiance* souhaité par la *RA* et ses *justificatifs* sont vérifiées. Si la vérification est positive, la *RA* enregistre l'*E-Identity*

correspondante. Si la vérification est négative, l'*E-Identity* ne peut être enregistrée avec le *niveau de confiance* souhaité.

  - Dans le cas d'auto-enregistrements (les *attributs* saisis par le *sujet* ne font l'objet que d'une vérification minimale), la présentation et la vérification de *justificatifs* peuvent être abandonnées. Les *attributs* peuvent être auto-déclarés.

- (conditionnel) Si le *sujet* souhaite représenter une *personne morale*, la RA doit vérifier le lien avec la *personne morale* au moyen de *justificatifs*. Si la vérification est positive, les *valeurs d'attribut* correspondantes sont demandées.
- (facultatif) La *RA* collecte des données afin de pouvoir attester de la présence du *sujet* en cas d'enregistrement ultérieur.
- Dans le cas d'auto-enregistrements (le *sujet* s'enregistre lui-même), la présentation et la vérification de *justificatifs* peuvent être abandonnées. Les *attributs* peuvent être auto-déclarés.
- Limite la durée de vie des *E-Identities* et soutient les *sujets* lors du renouvellement de leurs *E-Identities*.
- (facultatif) Associer des E-*Identities* (*Identity Linking*).
- Actualisation (pour la configuration de l'enregistrement par exemple) et désactivation des *E-Identities*. C'est à cette fin que l'on initie les processus suivants (*Définir les attributs* (**Fehler! Verweisquelle konnte nicht gefunden werden.**) et *Définir les moyens d'authentification* (**Fehler! Verweisquelle konnte nicht gefunden werden.**)).
- Soutient les *profiles* pour la séparation des responsabilités (Segregation of Duties, SoD).
- Toutes les actions et décisions prises sont enregistrées et documentées (Logging).

Remarques:

L'*E-Identity* constitue l'élément central de tout *système IAM*. Un *sujet* enregistré possède toujours au moins une *E-Identity* dans un *domaine*.

6.2.2 Définir les attributs

Définir les attributs	Saisie, mise à jour et suppression des *valeurs d'attribut*.

Propriétaire du processus: *AP*

Exigences: BP-6, FP-5, FP-6, Service-1, Dir-1

Activités:

- La condition préalable à la définition de *valeurs d'attribut* est la présence d'une *E-Identity* (*Définir l'E-Identity* **Fehler! Verweisquelle konnte nicht gefunden werden.**), à laquelle peuvent être affectées les *valeurs d'attribut*.

- Le *sujet* ou la *RA* du *CSP* sollicite, au cours de l'(auto)enregistrement, une nouvelle *valeur d'attribut* ou la mise à jour d'une v*aleur d'attributs* existante auprès de l'*AP*. La *RA* est compétente pour la vérification des *valeurs d'attribut*.
- (facultatif) La *RA* de l'*AP* collecte les *valeurs d'attribut* selon le niveau de qualité souhaité.
- Garantit de manière appropriée que les *valeurs d'attribut* sont bien à jour (il peut par exemple en limiter la durée de vie)
- (*RBAC* seulement) La *RA* peut assigner au *sujet* des *valeurs d'attribut* (de rôle), qui ont été allouées au sujet par le gestionnaire d'autorisation (*RBAC*/procédé basé sur une requête). Une *valeur d'attribut* correspondante est demandée.
- (facultatif) Le *sujet* peut transférer ses *droits* à un autre *sujet* pour une durée limitée et en fonction du contexte.
- L'*AP* assigne à l'*E-Identity* la *valeur d'attribut* ou met cette dernière à jour. On utilise à cet égard les définitions d'attribut pour le processus *Gérer la structure d'attribut* (6.3.3).
- L'*AP* supprime, le cas échéant, les *valeurs d'attribut*.
- Toutes les actions et décisions prises sont enregistrées et documentées (Logging).

Remarques:

Si les *attributs* décrivent toujours l'*E-Identity* correspondante, ils peuvent toutefois être fournis par le contexte commun aux *sujets* (un employeur commun par exemple). Ces *attributs* sont indépendants dans la mise à jour du cycle de vie de l'*E-Identity*. Seule la relation de l'*E-Identity* avec ces *attributs* est tributaire du «lifecycle» de l'*E-Identity*.

En fonction de l'organisation et du modèle d'Identity *Federation,* la *RA* peut être la même pour le *CSP* et l'*AP*. La *direction IAM* décide de la répartition des responsabilités.

Une *valeur d'attribut* représente une *propriété* attribuée à un *sujet*, qui décrit le *sujet* de manière plus approfondie. Le processus de collecte et de vérification de ces *propriétés* doit être documenté en fonction de la qualité exigée.

6.2.3 Définir les moyens d'authentification

Définir les moyens d'authentification	Création, délivrance et renouvellement de *moyens d'authentification* pour une *E-Identity.*

Propriétaire du processus: *CSP*

Exigences: BP-6, BP-8, BP-9, Service-1, Service-2, Dir-1

Activités:

- La condition préalable est qu'il y ait une *E-Identity* (*Définir l'E-Identity* **Fehler! Verweisquelle konnte nicht gefunden werden.**), à laquelle les *moyens d'authentification* peuvent être affectés.

- Le *CSP* crée, collecte et délivre des *caractères d'authentification* (mots de passe, certificat d'authentification par exemple) ou associe à l'*E-Identity* du *sujet* des *moyens d'authentification* dont ce dernier a déjà le contrôle. Un ou plusieurs *Credentials* sont créés et associés au *moyen d'authentification*.
- Le *CSP* veille à la confidentialité, l'intégrité et la disponibilité des *Credentials*.
- Les *Credentials* sont mis à la disposition du processus *Authentifier le sujet* (**Fehler! Verweisquelle konnte nicht gefunden werden.**).
- (facultatif) Le *CSP* utilise un gestionnaire de clés pour les clés cryptographiques.
- (facultatif) Le *CSP* publie les éléments publics des *moyens d'authentification* (clé publique par exemple) concernant l'*E-Identity.*
- Le *CSP* remet le *moyen d'authentification* (plusieurs le cas échéant) au *sujet* selon le niveau de confiance souhaité.
- Le *CSP* renouvelle ou remplace le *moyen d'authentification* de manière conviviale.
- Le *CSP* révoque le *moyen d'authentification*.
- Toutes les actions et décisions prises sont enregistrées et documentées (Logging).

6.2.4 Définir l'E-ressource

Définir l'E-Ressource	Identification, enregistrement et suppression d'*E-ressources*.

Propriétaire du processus: direction IAM (*RP*)

Exigences: BP-16, FP-1, FP-3

Activités:

- La *direction IAM* (*RP*) identifie les *ressources* et enregistre l'*E-Ressource* correspondante (avec *identifiant*). Une *ressource* peut être représentée par plusieurs *E-ressources*.
- (facultatif) La *direction IAM* (*RP*) classe les *E-ressources* en fonction de leurs besoins de protection en termes de confidentialité, d'intégrité et de disponibilité
- La *direction IAM* (*RP*) supprime ou désactive l'*E-Ressource*, ainsi que son *identifiant*. Toutes les actions et décisions prises sont enregistrées et documentées (Logging).

Remarques:

- Un *Relying Party* a toujours au moins une *E-Ressource* au sein d'un *domaine*.

6.2.5 Définir les règles d'entrée pour les E-ressources

Définir les autorisations pour les E-ressources	Affecter, mettre à jour et supprimer les *règles d'entrée* concernant l'*autorisation grossière* et les *droits d'accès* pour l'*autorisation précise* des *E-Identities* pour l'*accès* aux *ressources*.

Propriétaire du processus: *RP* ou *Broker*

Exigences: BP-17, FP-1, FP-4

Activités:

- Gérer les *règles d'entrée* en se servant des *attributs* disponibles des *E-Identities,* contexte de l'entrée (lieu, moment, *niveau de confiance* etc.).
- Affecter les *règles d'entrée* à une ou plusieurs *E-ressources*.
- Mettre à jour et supprimer les *règles d'entrée.*
- Toutes les actions et décisions prises sont enregistrées et documentées (Logging).
- (facultatif) Accède dans les *règles d'entrée* également aux besoins de protection de la *ressource* sollicitée (niveau de classification par exemple) ainsi qu'aux informations contextuelles (niveau de menace par exemple).

6.2.6 Définir les droits d'accès pour les E-ressources

Définir les autorisations pour les E-Ressources	Affecter, mettre à jour et supprimer les *droits d'accès* pour l'*autorisation précise* des *E-Identities* pour l'accès aux *ressources*.

Propriétaire du processus: *RP*

Exigences: BP-17, FP-1, FP-2, FP-2.1, FP-4

Activités:

- Le *RP* gère les *droits d'accès* en se servant des *attributs* disponibles des *E-Identities,* du contexte de l'accès (lieu, moment, *niveau de confiance* etc.) et, à titre facultatif, de ses propres données.
- Le *RP* alloue des *droits d'accès* à un ou plusieurs *E-ressources*.
- Le *RP* met à jour et supprime les *droits d'accès.*
- Toutes les actions et décisions prises sont enregistrées et documentées (Logging).

6.3 Diriger l'IAM (établissement)

En tenant compte des conditions générales organisationnelles de *Réguler IAM* et uniquement dans le cadre d'un contexte organisationnel, le processus administratif *Diriger l'IAM* contient les activités nécessaires pour atteindre les objectifs *IAM* définis, établir et gérer des processus administratifs (exécutants) et la «roadmap» pour la poursuite du développement du système IAM.

Ce processus décrivent le déroulement de la définition des directives requises et des conditions générales pour l'exploitation du système IAM, comme par exemple la définition de l'offre, la définition de règles et procédures, la détermination de la révision de l'exécution etc.

6.3.1 Diriger les prestataires de service

Diriger les prestataires de service	Etablissement, entretien et fin d'une relation avec les *prestataires de services IAM* du système IAM, y compris l'établissement de relations de confiance

Propriétaire du processus: *direction IAM* (système IAM global)

Exigences: Dir-5, Dir-5.1, Reg-1

Activités:

- Définir les *prestataires de services IAM* (*IdP*, *AP*, *CSP*, *RA*, *Broker*) à intégrer au groupement.
- Intégrer et supprimer les *prestataires de services IAM* (motif: End-Of-Life ou non-respect des consignes de sécurité par exemple).
- Gestion des contrats et/ou SLA Management avec les différents *prestataires de services IAM* ou acceptation des CGV en vigueur du *prestataire de services IAM*.
- Détermination de l'*organisation IAM* (rôles) et des relations entre participants (coopération).
- (conditionnel) Dans le cas où le *pilotage IAM* dans le processus *Gérer l'IAM Policy* (6.4.1) n'a pas stipulé le certificat approuvé, ce dernier doit être défini via la sélection de la Certificate Authority (CA).
- Détermination et mise à jour des *niveaux de confiance* pour l'*authentification*.
- (Facultatif) Détermination et mise à jour des niveaux de qualité des *attributs*.
- Analyse de l'impact des modifications sur les relations de confiance.

6.3.2 Diriger les Relying Parties

Diriger les Relying Parties	Etablissement, entretien et fin d'une relation avec les *Relying Parties (RP)*, y compris l'établissement de relations de confiance.

Propriétaire du processus: direction IAM (système IAM global)

Exigences: Dir-5, Dir-5.1, Reg-1

Activités:

- Contrôler l'intégration de *RP*, vérifier par exemple que les exigences en matière de sécurité sont bien respectées sur la base des besoins de protection.
- Gestion des contrats et/ou SLA Management avec les *RP*.

- Intégrer et retirer les *RP* du groupement (motif: End-Of-Life, développement de l'*E-Ressource* ou non-respect des consignes de sécurité par exemple). Initier le processus ***Fehler! Verweisquelle konnte nicht gefunden werden.*** (**Fehler! Verweisquelle konnte nicht gefunden werden.**).
- Contrôler les *attributs* nécessaires (présence et qualité) et, le cas échéant, initier le processus *Gérer la structure d'attente* (6.3.3).
- Analyse de l'impact sur les relations de confiance avant les modifications.
- (facultatif) Dans le cas où il y a plusieurs *domaines*, statuer sur l'appartenance

6.3.3 Gérer la structure d'attribut

Gérer la structure d'attribut	Définition et poursuite du développement de la définition des attributs.

Propriétaire du processus: *direction IAM* (système global) et *direction IAM* (AP)

Exigences: FP-7, Dir-1

Activités:

- Rechercher et vérifier les sources d'attributs.
- (conditionnel) Faute de source d'attributs, le processus doit être défini pour la *confirmation de valeur d'attribut* conformément au niveau de qualité souhaité.
- Définir, harmoniser et tenir à jour les méta-attributs et la sémantique.
- Classer les *attributs* (attributs personnes et d'entreprise par exemple).

6.3.4 Procéder au contrôle de l'exploitation

Procéder au contrôle de l'exploitation	Contrôler que le système IAM est correctement mis en œuvre et exploité.

Propriétaire du processus: *direction IAM*

Exigences: Reg-1, Reg-2

Activités:

- Inspecter et contrôler la mise en œuvre des directives, exigences de qualité, règles et règlementations.
- Rendre compte de toutes les activités pertinentes.
- Définir les mesures d'amélioration et/ou initier le processus ***Fehler! Verweisquelle konnte nicht gefunden werden.*** (**Fehler! Verweisquelle konnte nicht gefunden werden.**).

6.3.5 Gérer le catalogue des services IAM

Gérer le catalogue des services IAM	Créer et tenir à jour le catalogue des services IAM

Propriétaire du processus: *direction IAM* (système global) et *direction IAM* (*prestataires de service*)

Exigences: Service-3

Activités:

- Définir le service de stratégie IAM.
- Définir et tenir à jour le catalogue des services et les *architectures IAM* à réaliser.
- Analyse du marché pour l'exploitation des services (interne et externe)
- Feuille de route pour la poursuite du développement des *services IAM*.
- Echange d'informations et communication avec les *Relying Parties*.
- Sécurisation du financement pour l'exploitation et la poursuite du développement.
- Traitement des requêtes de poursuite du développement et, le cas échéant, initier le processus ***Fehler! Verweisquelle konnte nicht gefunden werden.*** (**Fehler! Verweisquelle konnte nicht gefunden werden.**).

6.3.6 Procéder à l'analyse des risques et surveiller les risques

Procéder à l'analyse des risques et surveiller les risques	Procéder aux analyses des risques et à l'évaluation des risques. Définir les mesures d'atténuation des risques et la surveillance des risques. Consigner les résultats.

Propriétaire du processus: *direction IAM*

Exigences: Reg-1, Reg-3

Activités:

- Procéder aux analyses des risques et consigner les résultats afin de permettre la détection rapide des dangers.
- Evaluation des risques et analyse des besoins de protection du système IAM: l'analyse des besoins de protection garantit des exigences de sécurité adaptées (autant de sécurité que nécessaire, par opposition à autant de sécurité que possible).
- Définir et initier des mesures d'atténuation des risques.
- Mettre en œuvre le concept d'information et de protection des données, ainsi que remontées à l'*IAM Regulator* concernant ce concept d'information et de protection des données.

- (Facultatif) Gestion des risques basée sur un système de gestion de la sécurité des informations (ISMS) selon ISO 27001, ISM3[8] ou selon ISO 31000 [6]. Gestion des risques basée sur un Framework comme COBIT [7].
- Concertation avec l'*IAM Regulator*.

6.3.7 Diriger la direction IAM

Diriger la direction IAM	Stipuler la collaboration des *directions* (*IAM*) dans le système IAM global.

Propriétaire du processus: *direction IAM* (système IAM global)

Exigences: Service-3, Dir-5

Activités:

- Stipulation de la coopération des *directions IAM* dans le système IAM global.
- Définition et amélioration continue des processus clé, de soutien et de direction.
- Création et mise à disposition de moyens de communication, adaptés aux différents échelons, pour divers Stakeholders.
- Détermination du serveur temporel.
- Définir, actualiser et révoquer les relations de confiance (Trust) entre les *prestataires de services IAM* et les *Relying Parties*. Déterminer comment les niveaux de qualité et de confiance sont transmis entre l'IdP/AP (ou *Broker*) et *RP*.
- Certification des *CSP*.
- Mise à jour et transférer des métadonnées aux *prestataires de services IAM* et *RP*.
- Gestion des *prestataires de services IAM* internes.
- Utilisation d'un *Logging Service* afin d'archiver les informations d'accès pour une traçabilité parfaite.

6.4 Réguler l'IAM (régulation)

En tenant compte des conditions générales organisationnelles et uniquement dans le cadre d'un contexte organisationnel, le processus administratif *Réguler l'IAM* contient les activités nécessaires pour définir les objectifs *IAM*, les conditions générales nécessaires et l'élaboration de schémas directeurs pour la gestion du *système IAM* global.

Ces processus définissent le déroulement de la définition des directives requises et des conditions générales pour la *direction* du système IAM, telles que la définition des règles et des procédures standardisées, la définition de la révision de la *direction*, etc.

[8] ISM3 est un ISMS qui peut être entièrement représenté selon la norme ISO 27001, mais qui, en outre, prend en compte la maturité de l'organisation.

6.4.1 Gérer l'IAM Policy

Gérer l'IAM Policy	Etablir l'*IAM Policy* et l'architecture *IAM* du système IAM.

Propriétaire du processus: *IAM Regulator*

Exigences: Dir-2, Reg-2, FP-11

Activités:

- Déduction et mise à niveau de la stratégie IAM.
- Définir l'architecture *IAM*.
- Définition des *acteurs* avec les tâches, compétences et responsabilité correspondantes.
- Elaboration des concepts de base nécessaires sur la base des *architectures IAM*, concept de types d'identité et concept de types de droit par exemple.
- Elaboration et mise à jour des directives pertinentes: identification des directives / règlementations légales, internes à l'entreprise et contractuelles en vigueur.
- Définir et mettre à niveau les documents auxiliaires pour l'application des architectures IAM et des directives. Calculateur de niveau de confiance par exemple.
- Définir les exigences de traçabilité, par exemple l'archivage des documents pertinents et les délais de conservation des données concernées (voir aussi ISO 29115 [8] Chapitre Record-keeping/recording).
- Définir les processus clé, de soutien et de direction standardisés pertinents. Spécialisation pour ce document.
- (facultatif) Etablir le certificat approuvé via la sélection de la Certificate Authority (CA). Ceci peut être déléguée à la *direction IAM*.
- Détermination du cycle de vie des *E-Identities*, *attributs*, *autorisations*, *prestataires de services IAM* et *RP*.
- (conditionnel) Détermination du cycle de vie d'une relation entre *personnes physiques et morales* (activation, suspension, renouvellement, révocation par exemple) (voir également eIDAS 2015/1502 [9], section 2.1.4).
- (facultatif) Etablir le modèle de maturité et les niveaux de maturité (selon eCH-0172 [10] par exemple).
- Etablir une procédure garantissant la définition et le respect des directives pour les participants d'une communauté (Baseline Requirements, Practice Statement et Compliance Report par exemple).
- Vérifier que les directives sont bien respectées. Contrôler les dérogations demandées par la *direction IAM*.
- .

6.4.2 Gérer le(s) modèle(s) de qualité

Gérer le(s) modèle(s) de qualité	Etablir la façon dont la qualité de l'*authentification* d'un *sujet* et la qualité des *attributs* peut être définie, vérifiée et comparée.

Propriétaire du processus: *IAM Regulator*

Exigences: Principe-5, IAM-1, FP-7, Reg-2

Activités:

- Définir le modèle de qualité pour l'*authentification* des *sujets*, de ses critères et leur subdivision (selon eCH-0170 [11]).
- Dans le cas où il y a des *attributs*, le modèle de qualité de *confirmations de valeur d'attribut*, de leurs critères et de leur subdivision doit être défini (selon eCH-0171 [5]).
- (facultatif) Etablir l'interopérabilité entre les modèles de qualité.

6.4.3 Réguler la gestion des risques

Réguler la gestion des risques	Etablir le contexte et identifier les risques. Quels risquent doivent être pris en compte de lors de l'établissement, la *période de définition*, la *période d'exécution* et le soutien ? Garde-fous pour la *direction IAM* concernant les risques à gérer.

Propriétaire du processus: *IAM Regulator*

Exigences: Dir-5, Reg-1, Reg-3

Activités:

- Définir les objectifs de sécurité IAM
- Etablir le contexte; l'établissement du contexte définit l'étendue de la gestion du processus de risque et stipule les critères à l'aune desquels sont évalués les risques.
- Définir combien de risques l'organisation est prête à prendre (propension au risque) et à combien de risques l'organisation peut-elle faire face (tolérance du risque)
- Procéder à l'identification des risques, selon ISO 31000 [6]. Vérification des plus importantes catégories de risques organisationnels, qui ont été prises en comptes lors de l'établissement du contexte, élaboration d'une vue d'ensemble avec les risques potentiels pouvant avoir un impact sur l'entreprise.
- Comparaison et intégration avec le système de gestion des risques pour l'organisation et ses objectifs.
- Elaboration du concept d'information et de protection des données (y compris les outils) en vue de son application par la *direction IAM*.
- Analyse des rapports de risque de la *direction IAM* et validation de ces rapports.

- Amélioration continue du concept d'information et de protection des données, comme pour ISO 27001 [12]. par exemple. En partant de la situation réelle, des possibilités d'amélioration sont identifiées périodiquement, le cas échéant, des mesures sont planifiées, appliquées et contrôlées sur la base de la propension au risque.
- Surveillance des cas d'incidents de sécurité externes connus/publiés et confier à la/ aux *direction(s) IAM* des missions d'évaluation des risques.
- (Facultatif) Soutien de la gestion des risques sur un système de gestion de la sécurité de l'information (ISMS) selon ISO 27001, O-ISM3[8] ou selon ISO 31000 [6] Soutien de la gestion des risque fondé sur Framework comme COBIT [7].

6.4.4 Diriger le pilotage IAM

Diriger le pilotage IAM	Intégration du pilotage IAM dans le système IAM global et la définition et l'amélioration continue des processus du pilotage IAM.

Propriétaire du processus: pilotage IAM

Exigences: Dir-5

Activités:

- Identification / établissement de la coopération des *domaines* de la *régulation* et de de la *direction*: dans le cas de la fédération, l'*IAM* s'étend en général à plusieurs *domaines*. L'organisation et les processus entre les *domaines* doivent être réglés de manière claire.
- Assurer une veille règlementaire et, le cas échéant, identifier les mesures en découlant.
- Déterminer les méthodes, notations, normes externes et cadres, qui doivent être appliqués dans le système IAM global.
- Garantit l'interopérabilité dans le système IAM global, concernant les méthodes, notations, etc.
- Amélioration continue de *Réguler l'IAM*. En partant de la situation réelle, des possibilités d'amélioration sont identifiées périodiquement, le cas échéant, des mesures sont planifiées, appliquées et contrôlées sur la base de la propension au risque.
- Effectuer les tâches d'assistance / habilitantes (en interne/ conditions générales), comme élaborer les conventions pour la documentation de l'*IAM Policy* et comparaison avec les conventions de l'organisation.

6.5 Soutenir l'IAM

En tenant compte des conditions générales organisationnelles et uniquement dans le cadre d'un contexte organisationnel, le processus administratif *Soutenir l'IAM* contient les activités nécessaires pour l'assistance, la mise en place et l'exploitation d'un système IAM. Il s'agit de processus supplémentaires, qui ne figurent pas dans le processus clé et de direction.

6.5.1 Soutenir les processus centraux

Soutenir les processus centraux	Le processus *Soutenir les processus centraux* englobe les activités pour intégrer, gérer, suivre et enfin résoudre les problèmes, qui peuvent survenir au cours de la *période d'exécution* ou *de définition*.

Propriétaire du processus: *IAM-Support*

Exigences: BP-12, BP-14, FP-9, Dir-4, Dir-6

Activités:

- Réception et traitement de cas problématiques en interaction entre le *sujet*, la *ressource* et tous les *prestataires de service* impliqués.
- Mise en place et exploitation d'un système de monitoring (pour la surveillance des événements, panne de service par exemple) et de tracking pour traiter et assurer le suivi des cas problématiques.
- Soutien et lancement de mesures dans le cas d'un événement revêtant une importance pour la sécurité (attaque informatique).
- Soutien en cas de soupçon d'utilisation abusive d'une E-Identity.
- Garantir l'interopérabilité de plusieurs systèmes de monitoring et de tracking.
- Intégrer les processus de soutien d'autres *prestataires de services IAM*.

6.5.2 Soutenir les processus de direction

Soutenir les processus de direction	Le processus *Soutenir les processus de direction* comprend les activités servant à soutenir et conseiller la *direction IAM* au cours de l'établissement.

Propriétaire du processus: IAM Support (Regulator)

Exigences: Dir-4

Activités:

- Communication et formation à l'*IAM Policy*.
- Elaboration de moyens de communication, adaptés aux différents échelons, pour les divers Stakeholders.
- (Facultatif) Soutien lors de projets IAM et projets spéciaux.
- Conseiller la *direction IAM*.

7 Services IAM

L'ensemble des services *IAM* proposés par les différents acteurs (voir chapitre 3.1) sont décrits ci-dessous. Il s'agit d'interfaces pour les processus (voir chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**) non de composants de services techniques; cela signifie que lors de la mise en œuvre, un ou plusieurs *services IAM* peuvent être implémentés par un composant de service technique, ou qu'un *service IAM* peut être distribué par plusieurs composants de service technique.

Les modèles de ce chapitre définissent aussi bien la *période d'exécution* (lorsqu'un *sujet* tente d'accéder à une *ressource*) que la *période de définition* pendant laquelle les différentes (méta)données sont saisies et tenues à jour. Les *services IAM* concernant les processus *Réguler l'IAM, Diriger l'IAM* et *Soutenir l'IAM* (voir chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**) ne sont pas présentés dans cette norme.

Dans les illustrations, les *services IAM* de la *période de définition* (en bleu clair) et les *services IAM* de la *période d'exécution* (en bleu foncé) sont séparés visuellement des objets du monde réel (en vert).

La *gestion de l'identité et des autorisations* des *services IAM* présentés ici ne fait pas partie de cette norme. En principe, toute utilisation d'un *service IAM* peut être différenciée par rapport aux objets du monde réel *Sujet* et *Ressource*, et la présente norme peut être appliquée de manière récursive. Il convient de déterminer au cas par cas si cela est judicieux dans la pratique.

7.1 Objets du monde réel

Les objets du monde réel et leurs tâches sont décrits de manière plus approfondie ci-dessous. Ils sont systématiquement affichés en vert clair dans les modèles.

.

7.1.1 Sujet

Sujet	Une *personne physique*, une *organisation agissante* ou un *service* ou une *chose*, qui a accès ou souhaite avoir accès à une *ressource*. Un *sujet* est représenté par des *E-Identities*.

Tâches (pour la période d'exécution):

- *S'authentifie*.
- (facultatif, pour les *personnes phys. uniquement*) Valide la *confirmation d'authentification* pour le *RP*.
- (facultatif, pour les *personnes phys. uniquement*) Valide l'envoi des *attributs*.
- Accède aux *ressources*.

7.1.2 Ressource

Ressource	Service ou données auxquelles un *sujet* peut avoir *accès* lorsqu'il s'est *authentifié* et que cela a été *autorisé* sur la base des *attributs* nécessaires.

Tâches (pour la période d'exécution):

- Met sa prestation technique (fonctionnalités) à la disposition du *sujet* (les informations et services correspondant à l'*identifiant*)

7.2 Services IAM pour la période de définition

La Figure 16 représente les *services IAM* pour la *période de définition* (en bleu clair dans les modèles) devant être utilisés pour la gestion des différents éléments d'information. Le premier groupe se réfère au *sujet*. Le deuxième groupe définit les éléments en relation avec la *ressource*.

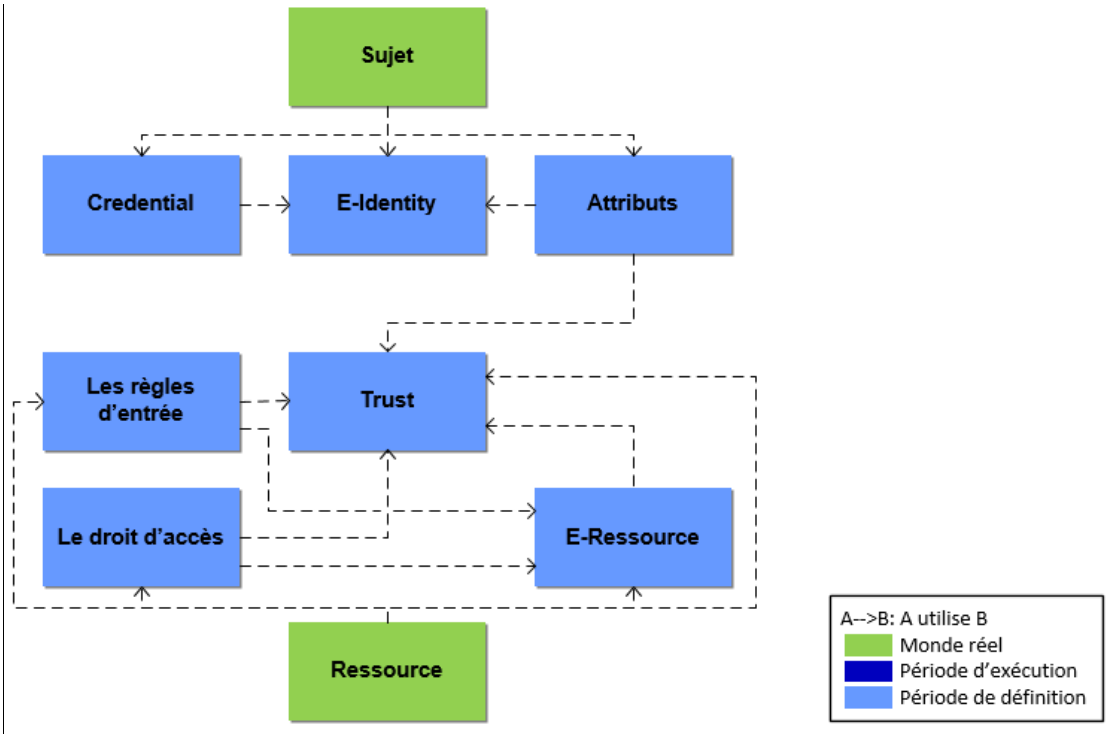


Figure 16 Services IAM – période de définition

7.2.1 E-Identity Service

E-Identity Service	L'*E-Identity Service* délivre des *E-Identities* aux *sujets* et les gère.

Processus: *Définir l'E-Identity* (**Fehler! Verweisquelle konnte nicht gefunden werden.**)

Interfaces:

In: *Sujet*,

(*E-Identities)*

Out: E-Identities

7.2.2 Credential Service

Credential Service	Le *Credential Service* délivre et gère les *moyens d'authentification*. Il permet de renouveler de manière conviviale ou de remplacer les moyens d'authentification. Un *moyen d'authentification* se réfère à une *E-Identity* et est délivré pour un *sujet* précis.

Processus: *Définir les moyens d'authentification* (**Fehler! Verweisquelle konnte nicht gefunden werden.**)

Interfaces:

In: E-Identity,

facteurs d'identification,

(moyen d'authentification)

Out: *moyen d'authentification, Credential*

7.2.3 Attribute Service

Attribute Service	L'*Attribute Service* maintient rapidement un ou plusieurs *attributs* actuels pour des *sujets* définis.

Processus: *Définir les attributs* (**Fehler! Verweisquelle konnte nicht gefunden werden.**)

Interfaces:

In: *E-Identity*, *propriétés du sujet*

Out: *Attributs*

7.2.4 Trust Service

Trust Service	Le *Trust* Service maintient les *prestataires de services IAM* et les *Relying Parties* acceptés et dignes de confiance.

Processus: *Diriger la direction IAM* (**Fehler! Verweisquelle konnte nicht gefunden werden.**)

Interfaces:

In: informations concernant qui fait confiance à qui concernant quoi,

métadonnées des *RP* et *prestataires de services IAM*,

métadonnées des *attributs* des *AP*

Out: Trust,

métadonnées des *RP* et *prestataires de services IAM*

7.2.5 E-Ressource Service

E-Ressource Service	L'*E-Ressource* Service délivre des *E-Ressources* concernant les *ressources* et les gère.

Processus: *Définir l'E-ressource* (**Fehler! Verweisquelle konnte nicht gefunden werden.**)

Interfaces:

In: *Ressource* d'un *Relying Party*

Out: *E-Ressource et métadonnées*

7.2.6 Service règles d'entrée

Service règles d'entrée	Le *service Règles d'entrée* gère les *règles d'entrée* pour une *E-Ressource*. Les règles sont définies sur la base de *l'authentification*, *d'attributs,* du contexte de l'*accès* (lieu, moment, *niveau de confiance* etc.) ou de propres modèles (groupes, rôles, autorisations individuelles).

Processus: *Définir les règles d'entrée pour les E-ressources* (**Fehler! Verweisquelle konnte nicht gefunden werden.**)

Interfaces:

In: Trust-relations,

E-ressources,

Type et qualité des attributs (métadonnées des *attributs*),

Type, qualité et contexte de l'*authentification*

Out: *Règles d'entrée*

7.2.7 Service Droit d'accès

Service Droit d'accès	Le *service Droit d'accès* gère les droits d'utilisation d'une *E-Ressource*. Les droits sont définis sur la base de *l'authentification*, des *attributs,* du contexte de l'*accès* ou des propres modèles (groupes, rôles, autorisations individuelles).

Processus: *Définir les droits d'accès aux E-ressources* (6.2.6)

Interfaces:

In: Trust-relations,

E-ressources,

Type et qualité des attributs (métadonnées des *attributs*),

Type, qualité et contexte de l'*authentification*

Out: *Règles d'accès*

7.3 Services IAM pour la période d'exécution

Les services IAM pour la période *d'exécution* (en bleu foncé dans les modèles) sont présentés dans la Figure 17. La figure comprend tous les *services IAM* qui sont utilisés pour le déroulement du processus de *contrôle de l'accès* pour la période *d'exécution*.

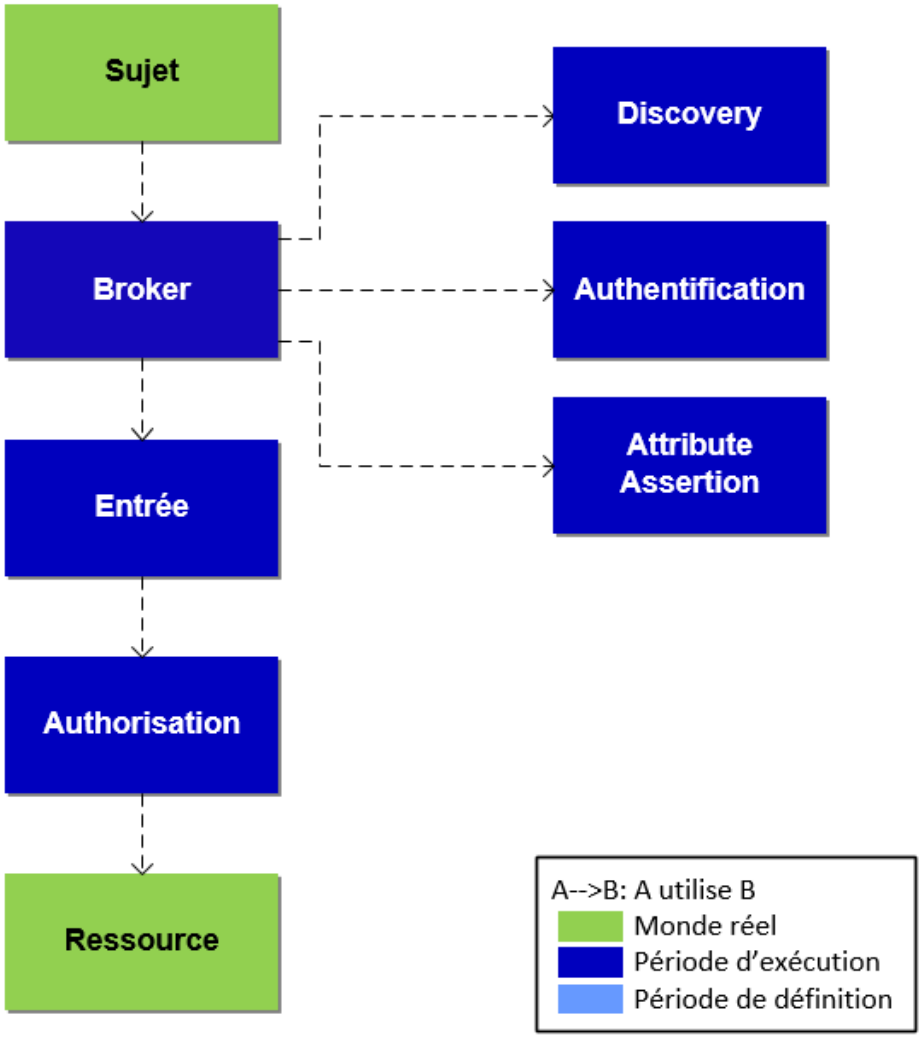


Figure 17 Services IAM – période d'exécution

7.3.1 Discovery Service

Discovery Service	Le *Discovery Service* propose une sélection d'IdP parmi lesquels le *sujet* peut choisir un *IdP*.

Processus: *IdP Discovery* (6.1.2)

Interface:

In: (*niveau de confiance* minimal requis)

Out: *IdP* choisi

7.3.2 Authentication Service

Authentication Service	L'*Authentication* Service vérifie à l'aide des *moyens d'authentification*, si celui qui accède (*sujet*) est celui qu'il prétend être.

Processus: *Authentifier le sujet* (**Fehler! Verweisquelle konnte nicht gefunden werden.**)

Interface:[9]

In: *requête d'authentification* (*Authentication Request)*,
(*identifiant)*,
facteurs d'identification

Out: *confirmation d'authentification* (indique si la vérification du *sujet* s'est révélée positive ou non),
(*identifiant*),
type et qualité de l'*authentification*

Nécessite: *Credential Service, Logging Service*

7.3.3 Attribute Assertion Service

Attribute Assertion Service	L'*Attribute Assertion Service* délivre des *confirmations d'attributs* à partir d'une interface définie.

Processus: *Enrichir l'E-Identity* (□)

Interface:

In: demande d'attribut (Attribute-Request),
identifiant,
(confirmation d'authentification)

Out: *confirmation d'attribut* (indique si la vérification de la relation entre un *attribut* et le *sujet* s'est révélée positive ou non).

Nécessite: *Attribute Service, Logging Service*

7.3.4 Broker Service

Broker Service	Ce *service IAM* l'intermédiaire entre le *sujet*, les *ressources* et les *services IAM* de la *période d'exécution*, fédère les *confirmations d'authentification* et *d'attribut*.

Processus: *Confirmer l'E-Identity* (**Fehler! Verweisquelle konnte nicht gefunden werden.**)

[9] Concernant les services pour la période d'exécution, les données requises en tant qu'informations pour la période d'exécution (In-Interface) ou disponibles une fois le service effectué (Out-Interface) sont indiquées dans l'interface. Si l'exécution nécessite des informations supplémentaires issues de la période de définition ou d'autres services de la période d'exécution, les services correspondants sont alors indiqués en conséquence (Need-Interface).

Interface:

In: (*niveau de confiance* minimal requis),
(*Identificateur),*
Trust

Out: *confirmations d'authentification,*
(confirmations d'attribut)

Nécessite: *Trust Service, Authentication Service, Attribute Assertion Service, Logging Service, E-Identity Service*

7.3.5 Service Entrée

Service Entrée	Le *service IAM* vérifie que les *règles d'entrée* sont bien respectées et accorde l'*entrée* au *sujet*, lorsque les règles correspondantes sont respectées.

Processus: *Autoriser l'entrée* (**Fehler! Verweisquelle konnte nicht gefunden werden.**)

Interface:

In: *Identificateur* d'une *E-Ressource, confirmations d'authentification et d'attribut*

Out: false ou true + *résultat d'authentification, (confirmations d'authentification et d'attribut)*

Nécessite: *Service règles d'entrée, Logging Service, Broker Service*

7.3.6 Authorisation Service

Authorisation Service	Le *service IAM* vérifie pour la période *d'exécution* que les *droits* d'utilisation de l'*E-Ressource* sont bien respectés et autorise l'utilisation de la *ressource* à un *sujet*, lorsque celui-ci possède bien les *droits* correspondants.

Processus: *Autoriser l'accès et Utiliser les attributs* (6.1.6)

Interface:

In: *confirmations d'authentification*,
confirmations d'attribut,
identifiant d'une *E-Ressource*

Out: Security Token (avec toutes les informations pertinentes pour l'*accès* à la r*essource*, en particulier les *confirmations d'attribut*)

Nécessite: *Service règles d'accès, Logging Service*

7.3.7 Logging Service

Logging Service	Le *service IAM* documente, pour la *période d'exécution* et de *définition,* l'utilisation d'un *service IAM* et met à la disposition de l'organisation de soutien les informations nécessaires à la résolution des problèmes d'utilisation ou des erreurs.

Processus: est contenu dans chaque processus de période d'exécution et de définition

Interface:

In: Données d'utilisation d'un *Service IAM*

Out: Logs

Nécessite: -

7.4 Modèle global

Tous les services *IAM* sont présentés simultanément dans la Figure 18 . On observe que les services pour la période d'exécution accèdent aux données des *services IAM* de la *période de définition* pour remplir leurs fonctionnalités. Dans un souci de clarté, il a été décidé de s'abstenir d'illustrer le service *Logging Services* pour la période d'exécution, qui est utilisé par tous les autres *services IAM*.

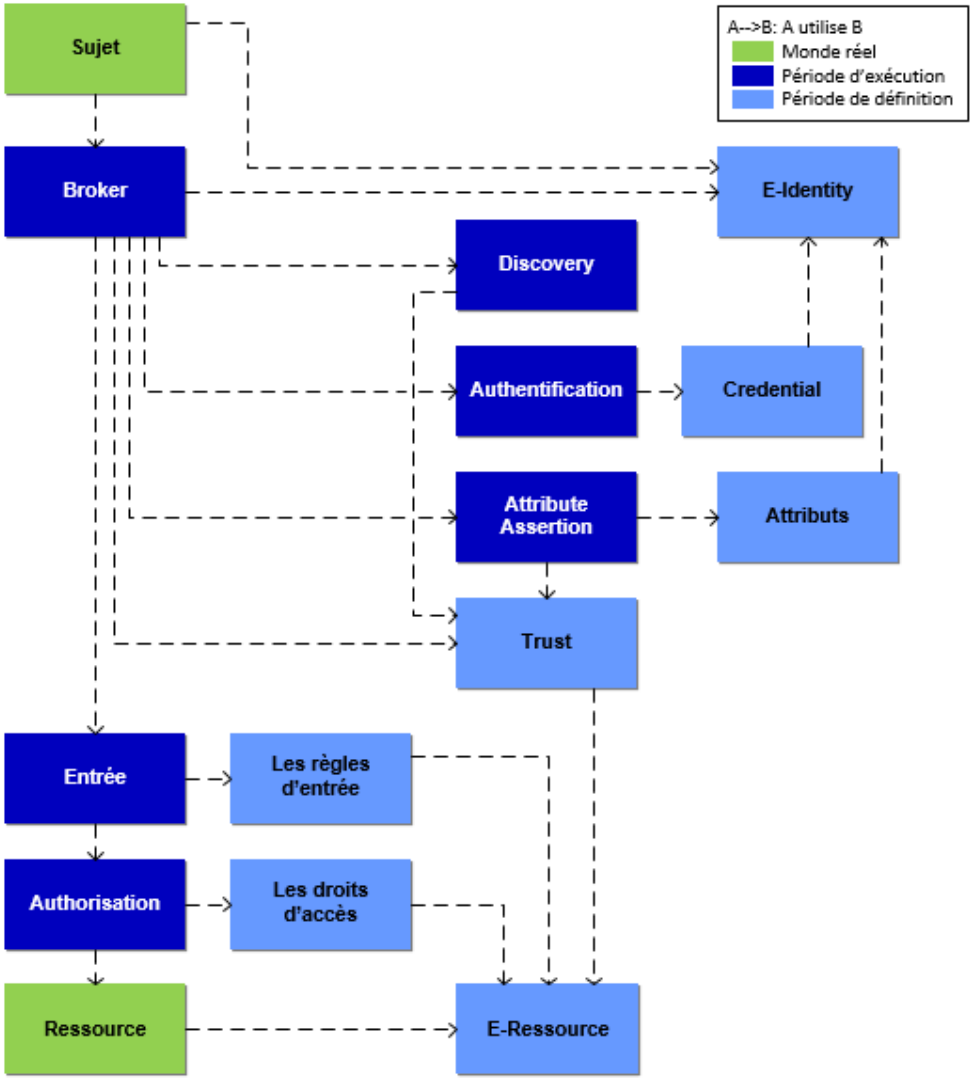


Figure 18 Services IAM – Vue d'ensemble

7.5 Soutien du processus par les services IAM

Cette partie présente comment les *services IAM* coopèrent entre eux à l'exemple des processus pour la période d'exécution. Cette collaboration entre les *services IAM* œuvrant à la réalisation des processus de définition est simple et déjà abordée directement dans les *services IAM* et dans la Figure 16. Ces processus ne sont donc pas présentés ici.

7.5.1 IdP Discovery

La Figure 19 illustre les utilisations des *services IAM* dans le cadre du processus *IdP Discovery* (6.1.2).

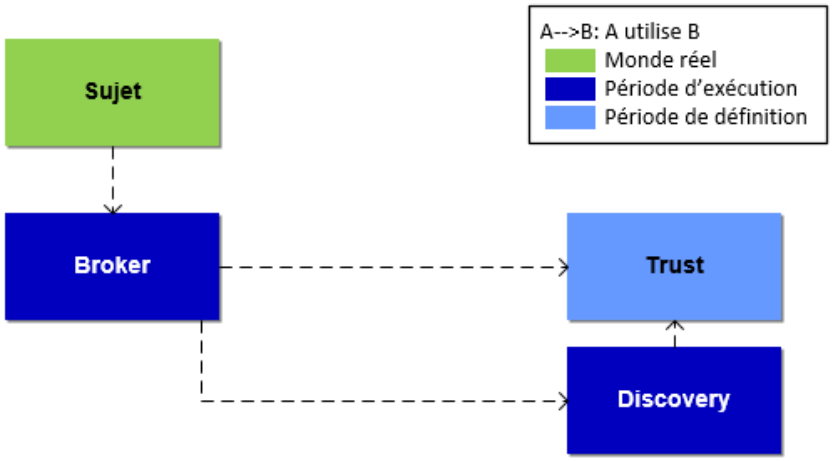


Figure 19 Soutien du processus *IdP Discovery*

IdP Discovery se déroule comme suit:

- Le *Broker Service* vérifie quel *Authentification Service* et (si nécessaire) quel *Attribute Assertion* Service selon le *Trust Service* remplit les exigences du service sollicitant et met une sélection à disposition.
- Le *sujet* choisit un *Authentification Service* (*IdP*) parmi la sélection proposée.

7.5.2 Authentifier le sujet

La Figure 20 illustre les utilisations de *Services IAM* dans le cadre du processus *Authentifier le sujet* (**Fehler! Verweisquelle konnte nicht gefunden werden.**).

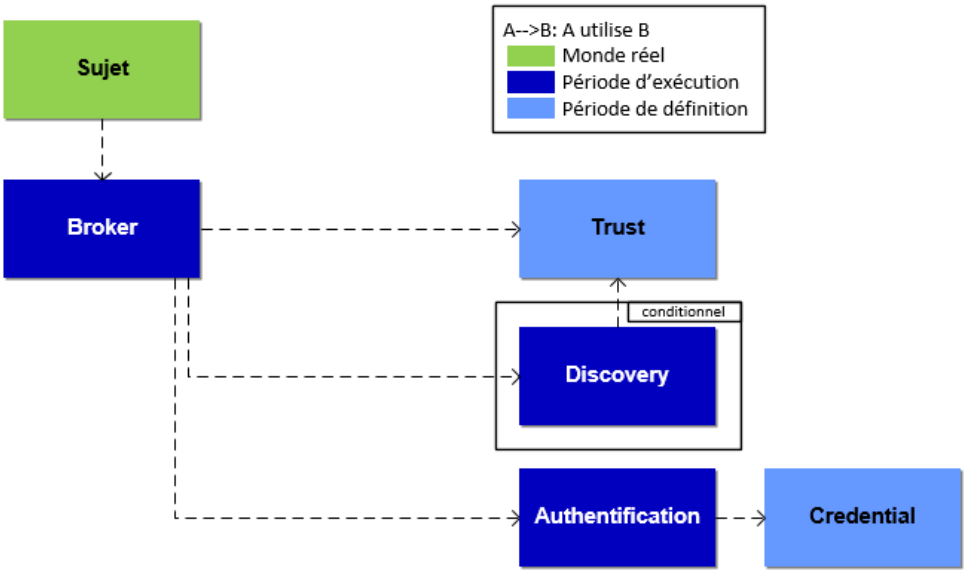


Figure 20 Soutien du processus *Authentifier le sujet*

Authentifier le sujet se déroule comme suit:

- Le *Broker Service* délègue l'*authentification* du *sujet* à l'*Authentification* Service choisi.
- Le *sujet* s'authentifie auprès de l'*Authentication* Service. Ce dernier contrôle la valeur d'émission générée de l'authentifiant par rapport au *Credential* de l'E-Identity supposée. Si cette vérification est positive, l'authentification a réussie.

7.5.3 Confirmer l'E-Identity

La Figure 21 illustre les utilisations des *services IAM* dans le cadre du processus *Confirmer l'E-Identity*.

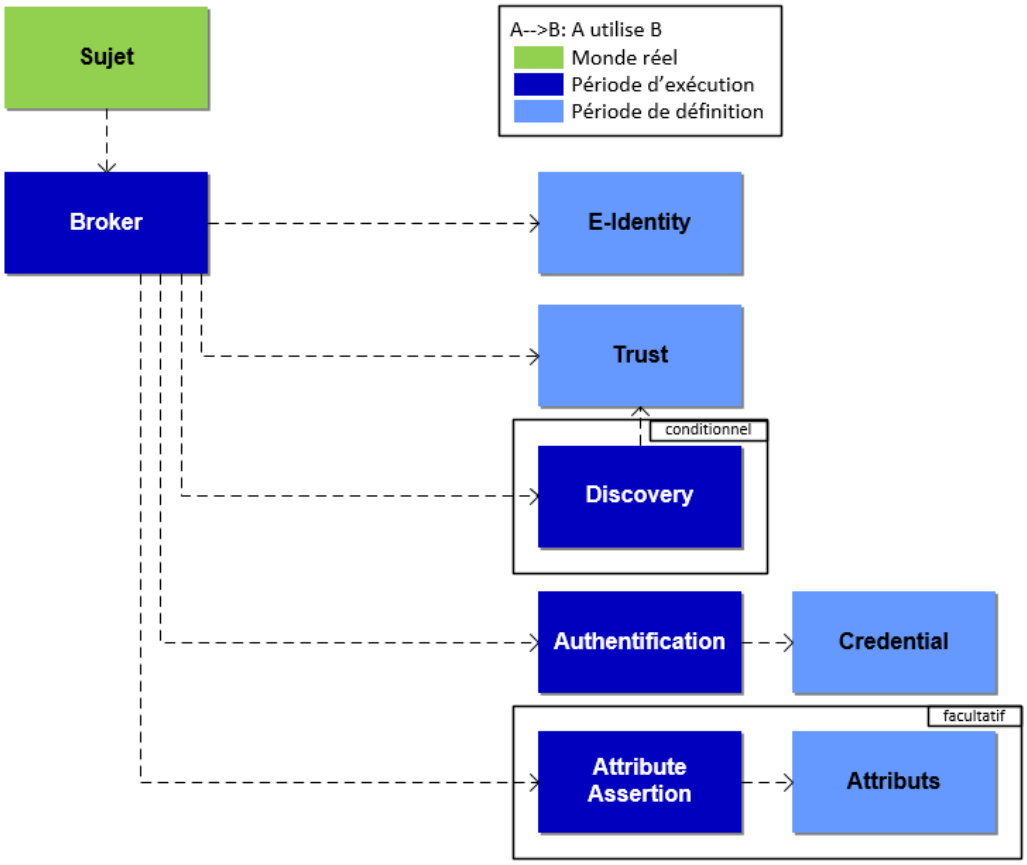


Figure 21 Soutien du processus *Confirmer l'E-Identity*

Confirmer l'E-Identity se déroule comme suit:

- Une fois l'authentification réussie, l'on vérifie si le service sollicitant a besoin des d'attributs.
- (facultatif) Dans le cas où des attributs sont nécessaires, la sélection de l'*Attribute Assertion* Service est alors réduite à ceux qui conduisent aux informations de l'*E-Identity* Service concernant l'*E-Identity,* conformément aux *E-Identities* (linkedID) reliées.
    - L'E-Identity est enrichie d'attributs selon le *service IAM Enrichir l'E-Identity (voir section* ***Fehler! Verweisquelle konnte nicht gefunden werden.****)*.
- Le *Broker Service* génère la confirmation de l'authentification et de l'attribut et la transmet au service sollicitant

7.5.4 Enrichir l'E-Identity

La Figure 22 illustre les utilisations des *services IAM* dans le cadre du processus *Enrichir l'E-Identity*.

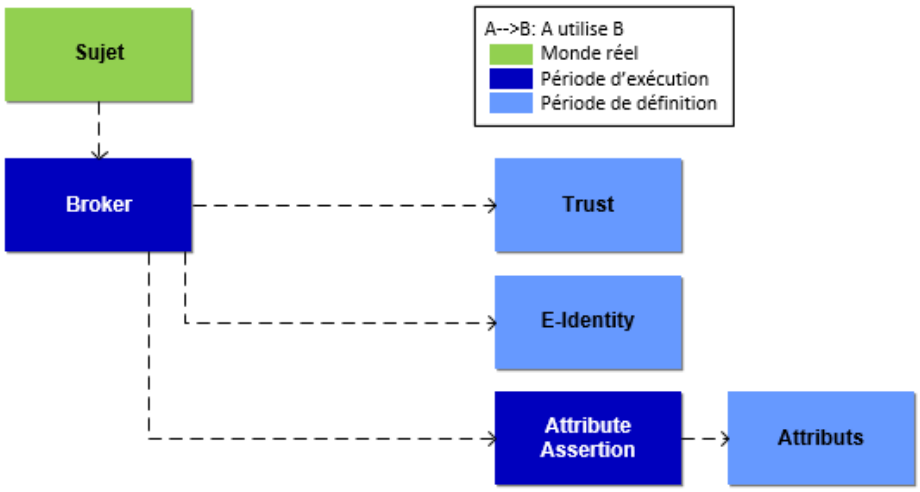


Figure 22 Soutien du processus *Enrichir l'E-Identity*

Enrichir l'E-Identity se déroule comme suit:

- Le *Broker Service* demande à l'*Attribute Assertion* Service concerné de confirmer les *attributs* correspondants.
- (facultatif) Le *Broker Service* obtient du sujet la confirmation (personnes physiques uniquement) du résultat de l'authentification et de transmettre les attributs déterminés au service sollicitant.

7.5.5 Autoriser l'entrée

La Figure 23 illustre les utilisations des *services IAM* dans le cadre du processus *Autoriser l'entrée.*

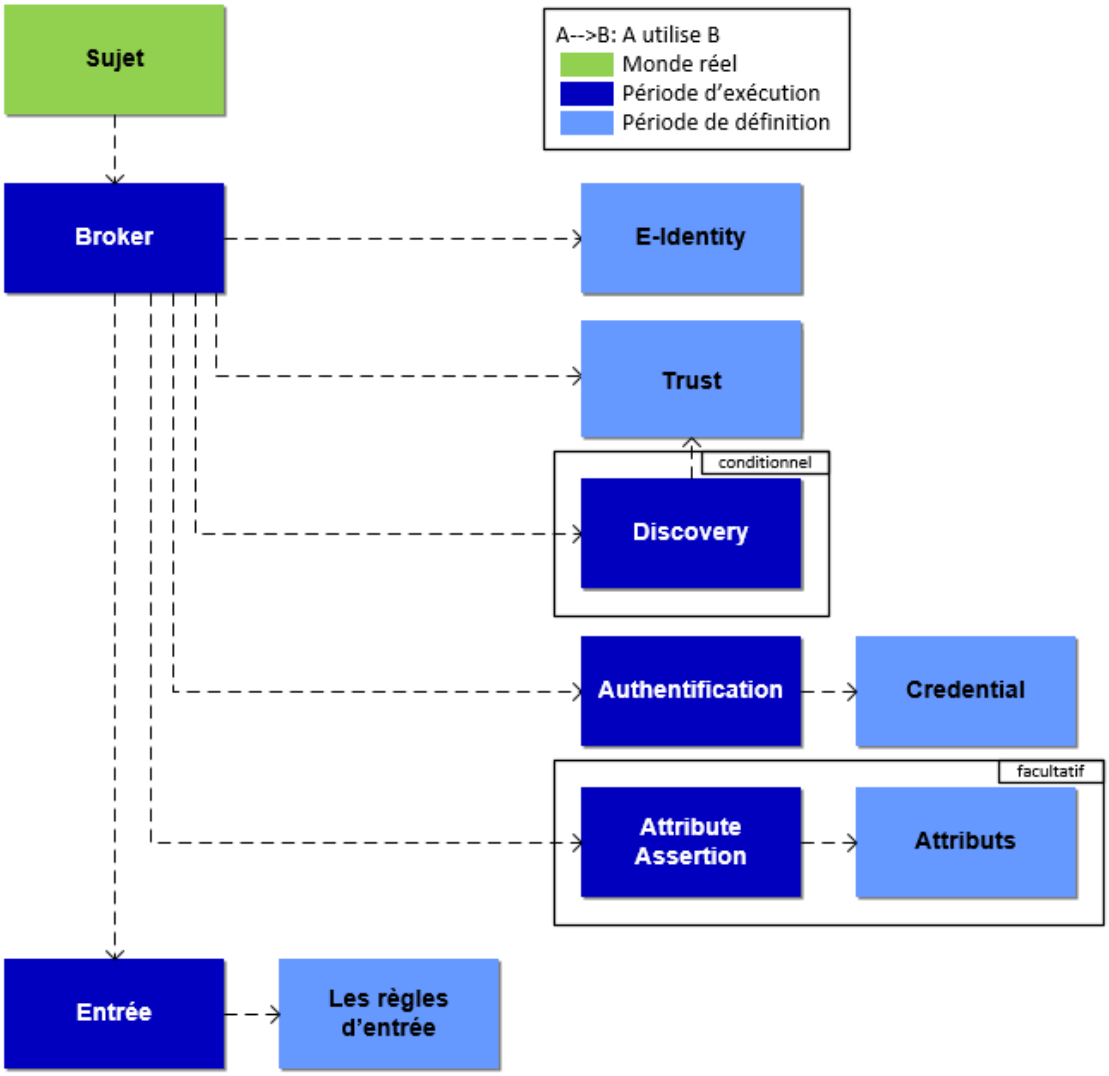


Figure 23 Soutien du processus *Autoriser l'entrée*

Autoriser l'entrée se déroule comme suit:

- Le *service d'entrée* vérifie les règles d'entrée pour cette E-Ressource et exige du *Broker Service* qu'il authentifie le sujet et confirme les attributs relatifs à l'*E-Identity* conformément aux exigences (voir sections **Fehler! Verweisquelle konnte nicht gefunden werden.** et **Fehler! Verweisquelle konnte nicht gefunden werden.**)
- Le *service d'entrée* vérifie le droit d'entrée sur la base des *confirmations d'authentification et d'attribut.*
- Le *service d'entrée* accorde l'*entrée* à la *ressource* et transmet les *confirmations d'authentification et d'attribut.*

7.5.6 Autoriser l'accès et utiliser les attributs

La Figure 24 illustre les utilisations des *services IAM* dans le cadre du processus *Autoriser l'accès et utiliser les attributs* (6.1.6).

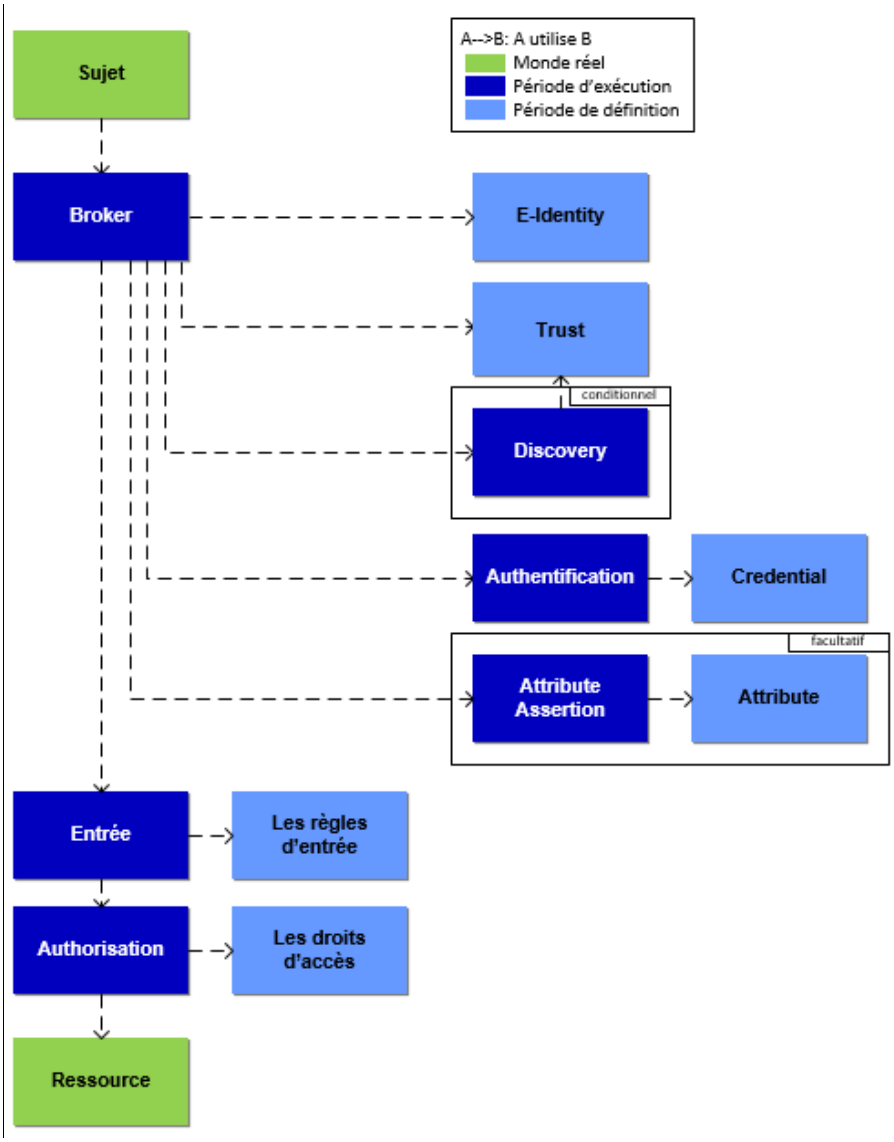


Figure 24 Soutien du processus *Autoriser l'entrée et Utiliser les attributs*

Autoriser l'accès et utiliser les attributs se déroule comme suit:

- *L'Authorisation Service* vérifie les *droits d'accès* pour cette *E-Ressource* et exige du *service d'entrée* les *confirmations d'authentification* ou *d'attribut* correspondantes.
- *L'Authorisation Service* vérifie le *droit d'accès* sur la base des *confirmations d'authentification et d'attribut, du* contexte de l'*accès* ou de propres modèles (groupes, rôles, autorisations individuelles).
- *L'Authorisation Service* accorde l'*accès* à la *ressource* et transmet les *confirmations d'authentification et d'attribut.* Les *attributs* peuvent à présent être utilisés en conséquence.

7.6 Attribution des services aux éléments d'information

Le tableau suivant illustre la relation entre les *services IAM* et les éléments de l'architecture de l'information (sémantique et interface). Les *services IAM* de la *période de définition* traitent (B) les objets et leurs relations réciproques. Les *services IAM* de la *période d'exécution* lisent (L) les objets et leurs relations réciproques. Toutefois, les différents *services IAM* utilisent uniquement les *métadonnées* (M) d'autres *services IAM*.

		Elément d'information										
		E-Identity[10]	**Attribut**[11]	**Règles d'entrée**	**Droit d'accès**	**E-Ressource**	**Credential**	**Identifiant d'une E-Identity**	**de l'authentifiant**	**Confirmation d'authentification**	**Confirmation d'attribut**	**Identifiant d'une E-Ressource**
Services IAM	E-Identity	B	B[12]					B				
	Credential	L					B	L				
	Attributs	L	B					L				
	Trust	M	M			M						
	E-Ressource					B						B
	Règles d'entrée	M	M	B		L						
	Droit d'accès	M	M	L	B	L						
	Authentication	L					L	L	B			
	Attribut Assertion		L					L		L	B	
	Broker	L						L	L	BP[13]	BP[13]	
	Entrée			L		L		L		L	L	L
	Autorisation				L	L		L		L	L	L

B = Traiter (Create/Read/Update/Delete), L = Lire (Read), M = ne lit que les métadonnées

Tableau 5 Relation entre les services IAM et la sémantique du modèle d'information

[10] y compris la relation avec *linkedID*
[11] y compris la relation avec l'*E-Identity*
[12] B pour *identifiant* (est également un *attribut*)
[13] B, quand le Broker Service délivre lui-même des *confirmations d'authentification et d'attribut* combinées

7.7 Compétences pour les services IAM

Le Tableau 6 démontre quels Stakeholders proposent idéalement quel type de *service IAM* pour la *période de définition et d'exécution*. Les *services IAM* sont décrits de manière plus approfondie dans le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**. La répartition proposée ici optimise la réutilisation des *services IAM* dans une *Identity Federation*. C'est pourquoi le *Relying Party* confie autant de responsabilité organisationnelle que possible aux *prestataires de services IAM*.

		Stakeholders					
		Prestataire de services IAM					Relying Party
		IdP	AP	CSP	RA	Broker	
Service IAM	E-Identity				X		
	Credential			X			
	Attributs		X				
	Trust					X	
	E-Ressource						X
	Règles d'entrée					X	
	Droit d'accès						X
	Authentication	X					
	Attribute Assertion		X				
	Broker					X	
	Entrée					X	
	Autorisation						X

Tableau 6 Relation entre les services IAM et les Stakeholders

8 IAM pour l'IoT

Une *chose* dans le présent contexte est un objet physique, qui communique de manière active et autonome avec les *ressources* via un *réseau*[14]. Plusieurs *choses* connectées par un même *réseau* forment un *Internet of Things* ou IoT (Internet des objets en français). Les robots, les éléments actifs de l'automatisation des bâtiments, les voitures modernes (qui se conduiront toutes seules à l'avenir) ou, plus généralement, les nœuds de toutes sortes de capteurs en sont de bons exemples.

Le concept d'IoT remonte aux années 1980. Si les *choses* capables d'agir de manière autonome existent depuis bien longtemps (systèmes d'alerte par exemple), l'IoT va connaître son véritable essor avec l'avènement de la miniaturisation et de l'automatisation des systèmes de fabrication, de transport et de commande.

Il est encore trop tôt pour évaluer les répercussions à long terme de l'IoT sur les principes de conception de la *gestion des identités et des accès (IAM)*. Ce chapitre traite des domaines dans lesquels de telles répercussions sont à prévoir.

Par principe, c'est au Regulator qu'il incombe de définir la façon dont les *choses* doivent être gérées dans un *système IAM fédéré*. La Life-Cycle Management (gestion du cycle de vie) et le concept de sécurité des *choses* sont également concernés.

Les *choses* sont considérées comme des *sujets* dans le cadre de cette norme. Si les choses sont considérées comme des *ressources*, il n'y a aucune particularité par rapport à une *ressource* ordinaire.

8.1 Propriétés spéciales des choses

Les *choses* (ou things) sont des objets du monde réel qui accèdent aux *ressources*. Dans l'architecture de l'information de la présente norme, elles sont représentées en tant que *sujets* ayant une *propriété* spécifique. Elles se distinguent en particulier des *personnes physiques* par les points suivants:

- Les *choses* peuvent appartenir à une *personne physique* ou à une *organisation*, appelée propriétaire (de la *chose*) dans la suite du document. Le propriétaire est responsable de ses *choses* et répond de leurs activités dans l'IoT[15].
- Outre la «possession», d'autres relations entre *choses* et *sujets* peuvent également être importantes pour la gestion des identités et des accès des choses («fabriqué par» ou «utilisé par» par exemple).

[14] Dans la littérature, une *chose* est parfois désignée par le terme objet (object en anglais). Le terme «objet» étant déjà chargé de sens (utilisations dans d'autres domaines), la désignation *chose* a été privilégiée. La désignation de l'identifiant d'une chose est souvent «oid».

[15] Le cas échéant, le fabricant de la chose peut aussi être appelé à en répondre. Ce point ne sera toutefois pas traité plus avant ici.

- Les *choses* peuvent utiliser uniquement les données disponibles sous forme électronique. Toutes les données pertinentes pour la période *d'exécution*, tels les *facteurs d'identification* (PIN par exemple) et les décisions (validation d'*attributs* par exemple), doivent donc être configurées pour la période *de définition*.
- Les *choses* sont fréquemment composées d'autres *choses* comme un bâtiment, qui contient des ascenseurs, qui comprennent pour leur part un système d'alerte par exemple. Ou un véhicule avec un ordinateur de bord équipé d'un GPS et d'un tachygraphe.
- Les *choses* peut avoir une durée de vie très différente, de quelques heures (voire minutes) à de nombreuses années.
- Le nombre de *choses* n'est pas limité dans le temps. On estime de 1'000 à 5'000 la quantité de choses par personne. La gestion échelonnable des *choses* nécessite un niveau d'automatisation avancé.

8.2 Impact sur l'architecture d'information IAM

Les *services IAM* peuvent en principe être appliqués également aux *choses*.

Compte tenu des propriétés particulières des *choses*, différents aspects sont à prendre compte lors de la mise en œuvre. Bon nombre de ces aspects portent sur l'architecture de l'information IAM et, plus spécifiquement, sur la gestion des relations complexes entre les *sujets*:

Aspect	Principe, description et mise en œuvre dans l'IAM
Possesseur[16]	Les *choses* dans l'IoT devraient toujours avoir un possesseur. La possession peut être limitée (location de voiture ou de logements de villégiature par exemple) ou permanente jusqu'à révocation (situation ordinaire). Certaines *choses* peuvent également avoir plusieurs possesseurs (un réfrigérateur qui effectue des commandes de réapprovisionnement alimentaire pour tous les habitants d'une colocation par exemple). Le concept de «possesseurs» (de *choses*) implique une relation supplémentaire dans le cadre de l'architecture de l'information (comparer à cet égard la définition du *sujet* dans l'architecture de l'information). *Remarque*: cette relation complémentaire peut, le cas échéant, être aussi utilisée indépendamment de l'IoT afin de gérer les dépendances entre les *sujets* (gestion des *E-Identities* séparées pour les activités d'administrateur informatique par exemple).

[16] Le thème de l'IoT étant relativement nouveau dans le monde de l'informatique, la distinction juridique entre propriétaire et possesseur n'est pas abordée dans ces pages.

Accès «On behalf» (au nom de)	Les *choses* utilisent les *ressources* «on behalf» de leur possesseur. La voiture recherche une place de stationnement libre ou une station-service, le téléphone portable met à jour les données locales, le réfrigérateur commande du lait. Ceci implique la possibilité qu'une *personne physique* ou une *organisation* puisse transférer, de manière temporaire ou permanente, les *attributs* de son *E-Identity* aux *E-Identities* de ses *choses*.
Attributs propres et transférés	Les *choses* ont des *attributs* propres et transférés. Les *attributs* propres sont inhérents d'un point de vue statique (numéro de série, date de production par exemple) ou dynamique (emplacement actuel, consommation actuelle, clé d'authentification actuellement active par exemple). Les *attributs* transférés proviennent du possesseur, comme son appartenance à une organisation, son adresse postale ou ses coordonnées bancaires par exemple. Les règles doivent être définies concernant le transfert d'*attributs* à des *choses*. Exemples de règles relatives au transfert: • Les *attributs* peuvent être transférés uniquement par des *personnes physiques* (cas des *organisations*: par un représentant spécialement habilité). • Il est évident qu'un *attribut* a été transféré et par qui. • Les *attributs* transférés ont été retirés, dès qu'ils ont été retirés au transférant. • Lors du transfert d'un *attribut*, il est défini si le transfert fonctionne également de façon «transitive» (c'est notamment le cas des *choses* assemblées) (le GPS d'un véhicule par exemple. Celui-ci peut-il transmettre l'attribut «modèle de véhicule»?).
Changement de possesseur	Les *choses* peuvent changer de possesseur. Les *choses* à longue durée de vie (ex.: biens d'investissement) peuvent changer plusieurs fois de possesseur au cours de leur durée de vie. Les *attributs* propres (inhérents et dynamiques) restent inchangés lors d'un changement de possesseur. Les *attributs* transférés doivent être supprimés et, le cas échéant, transférer de nouveau par le nouveau possesseur. Il faut en outre s'assurer qu'il y a bien un possesseur défini à chaque instant.
Remplacement de choses	Les *choses* peuvent être remplacées. Les choses ayant une durée de vie courte (ex.: consommables) peuvent être remplacées 1:1. Les *attributs* propres (inhérents et dynamiques) sont redéfinis en cas de remplacement. Les *attributs* transférés doivent pouvoir être automatiquement transférés à la *chose* de remplacement.

Choses composées	Les *choses* peuvent être composées de *choses*. Les *choses* complexes sont composées de *choses*, aucune restriction n'étant imposée en termes de degré d'imbrication. Une *chose* peut même appartenir à plusieurs *choses* assemblées comme par exemple un compteur électrique intelligent, qui appartient à la fois au bâtiment et au groupe régional d'exploitation du réseau électrique. L'IAM doit être en mesure de représenter également les relations complexes entre les *choses*, de sorte à permettre l'ajout et la suppression de choses.

8.3 Impact sur les services IAM

Les propriétés particulières des *choses* ont également un impact sur les *services IAM*:

Aspect	Principe, description et mise en œuvre dans l'IAM
Moyen d'authentification intégré	Les *choses* peuvent présenter un *moyen d'authentification* intégré. Pour qu'une *chose* puisse être active de manière autonome et sans l'intervention manuelle d'une *personne physique*, toutes les données requises pour l'*authentification* pour la période *d'exécution* doivent être disponibles sous forme électronique. Cela concerne en particulier les clés cryptographiques avec les données d'activation correspondantes (PIN par exemple). L'*Authentication Service* pour l'*authentification* des *sujets* doit tenir compte des *propriétés* spécifiques des *choses*.
Enregistrement automatique, y compris inventaire	Les *choses* peuvent s'enregistrer de manière automatique. La gestion du nombre – vraisemblablement très important à long terme – de *choses* nécessite des processus de gestion pour la plupart automatisés. Cela concerne en particulier l'enregistrement et l'inventaire des *choses* à mesure qu'elles intègrent l'Internet of Things (ou qu'elles en ressortent ultérieurement). L'*E-Identity Service* et le *Credential Service* doivent tenir compte des *propriétés* spécifiques de *choses* et, en particulier, permettre l'automatisation.

9 Respect de la vie privée

Ce chapitre décrit les exigences concernant la protection de la vie privée du *sujet*, sortant du cadre des exigences se rapportant au sujet, exposées au chapitre 4.3.1. La protection de la vie privée est déterminante pour la confiance dans le système IAM, en particulier pour les scenarii impliquant le recours par la population à des *ressources* officielles et administratives (scenarii C2G).

Le *Regulator* est responsable de la définition et du respect des exigences propres à la protection de la vie privée. Il lui incombe de communiquer de manière transparente avec tous les participants au sujet des mesures prises.

9.1 Exigences en matière de sécurité et concernant la protection de la vie privée

Cette section répertorie les exigences générales en matière de sécurité et concernant la protection des données personnelles d'un *sujet* dans un *système IAM fédéré*. En fonction des conditions générales et du modèle *d'Identity Federation* sélectionné, les exigences souhaitées devraient être prises en compte lors de la mise en œuvre. Cette remarque s'applique tout particulièrement aux modèles incluant un *Broker* central.

ID	Définition	Exigence	Application dans l'IAM fédéré
R1	**Intraçabilité (Untraceability)**	Un *sujet* peut accéder à une *ressource* ou à un service, sans que d'autres participants au système puissent le constater.	Un système, qui est impliqué dans une opération d'authentification, ne doit pas pouvoir constater sans une tierce-partie si et quand un *sujet* a utilisé une *ressource* ou un autre service.
R2	**Inobservabilité (Unobservability)**	Un *sujet* peut accéder à une *ressource* ou à un service, sans qu'un tiers non-autorisé puisse le constater.	Un système, qui n'est pas impliqué dans une opération d'authentification, ne doit pas pouvoir constater (en surveillant les opérations de communication ou par corrélation temporelle par exemple), si et quand un *sujet* particulier a utilisé un service.
R3	**Inassociabilité (Unlinkability)**	Un utilisateur peut accéder à plusieurs reprises à une *ressource*, sans que les participants au système ou un tiers non autorisé puissent associer ces événements.	Un *sujet* doit pouvoir accéder à différents *RP* de manière répétée, sans que son identité puisse être découverte par les systèmes impliqués ou par un tiers (par corrélation des *identifiants* transmis par exemple).

R4	**Confidentialité (Confidentiality)**	Les informations sensibles ou permettant d'identifier les personnes ne doivent pouvoir être consultées que par les systèmes autorisés et par le *sujet* lui-même.	Un système, qui est impliqué dans une opération d'authentification et qui n'est pas digne de confiance, ne doit pas pouvoir consulter des informations relatives à l'identité (*attributs* transmis) et/ou constater l'identité du *sujet* (par un chiffrage ‚*end-to-end*' par exemple).
R5	**Authenticité et intégrité des données (Authenticity & Integrity)**	Un *RP* peut contrôler l'origine, l'authenticité et l'intégrité d'informations relatives à l'identité d'un *sujet* jusqu'à sa source.	Un *RP* peut déterminer si une *confirmation de l'authentification et de l'attribut* provient de la source d'autorité attendue et connue d'elle.
R6	**Approbation/transmission (Consent)**	La transmission d'informations relatives à l'identité à un service sollicitant ne peut se faire sans l'accord du *sujet*.	L'approbation de la transmission d'informations identifiant les personnes est obtenue auprès du *sujet* par un système compétent à cet égard (*Broker*, *IdP* ou *AP*). L'approbation porte également sur l'utilisation prévue pour les données.
R7	**Droit à l'information (Right to Information)**	Une instance traitant les données doit pouvoir à tout moment tenir informé un *sujet* des données qu'elles traitent et qui concernent ce *sujet*.	Les systèmes, qui sont impliqués dans une opération d'authentification, doivent pouvoir, à tout moment, fournir des informations concernant les données concernant un *sujet*, qui ont été saisies, traitées, associées, enregistrées et transmises.
R8	**Autorisation de demande (Request Permission)**	Seuls les systèmes dûment autorisés sont habilités à demander des informations concernant un *sujet*.	Un RP ne peut demander des informations concernant un *sujet* que si elle y est autorisée.
R9	**Traçabilité (Auditability)**	Les informations transmises dans le cadre d'une opération d'authentification particulière et les *métadonnées* correspondantes doivent être disponibles.	Les informations transmises relatives à l'identité et les *métadonnées* correspondantes peuvent être consultées au niveau central ou compilées a posteriori avec le concours de toutes les entités impliquées.

Tableau 7: Exigences concernant la protection de la vie privée

9.2 Gestion et traitement des données de sujets

Ce chapitre propose une directive sur les points à prendre en compte lors de la gestion et du traitement des données du *sujet*. La principale condition préalable est que l'utilisateur puisse s'assurer à tout moment de la manière dont ses données sont utilisées. Cette section décrit les mesures à prendre en compte et dans quels scenarii pour la protection des données. Elle a vocation à rendre les *prestataires de services* plus dignes de confiance.

Minimisation de la collecte des données et du volume de données

La *RA* est autorisée à collecter les *attributs* identifiant le sujet à des fins d'identification et de vérification d'un sujet.
Un *Broker* n'est autorisé à transmettre à un *RP* que les *attributs* explicitement demandés par le *RP*. Dans les cas particuliers, il n'est pas nécessaire de divulguer les *attributs* dans leur intégralité. Par exemple, lorsque le *RP* souhaite savoir uniquement si le *sujet* a 18 ans ou plus, la date de naissance explicite ne devrait pas être transmise.
En outre, un *RP* n'est autorisé à demander, à propos d'un *sujet,* que les *attributs* dont il a besoin pour remplir sa fonction. Demander des attributs inutiles peut miner la confiance.

Empêcher le profilage

L'association de données, permettant de remonter jusqu'à un *sujet*, devrait être réduite au minimum. Des mesures organisationnelles et techniques devraient être prises afin d'empêcher que des profils de personnalité ne soient créés.
Le Regulator définit les mesures organisationnelles et techniques pour le système IAM et devrait les publier aux autres acteurs.

Prise de connaissance et validation

Le *sujet* doit toujours être mis au courant de quels *attributs* sont utilisés et sous quelle forme. La transmission d'*attributs* (en cas de fédération par exemple) est autorisée uniquement après que le *sujet* y a consenti explicitement au moins la première fois.

Restriction d'utilisation

Un *prestataire de services* doit pouvoir, à tout moment, indiquer de manière transparente quelles données ont été sollicitées et traités et pour quels motifs[17]. Les données permettant d'identifier le sujet ne doivent pas être transmises à un tiers sans le consentement du *sujet*, sauf si la loi en décide autrement.

Analyse de la protection des données et des risques

Les analyses de la protection des données et des risques doivent aider à estimer les besoins de protection d'une *ressource* et à concevoir les mesures correspondantes afin de garantir la protection des données selon les dispositions légales et la pratique habituelle.

Mesures de protection des données

Les mesures élaborées en vue de protéger les données doivent préserver la fiabilité des *prestataires de service*. Les mesures de protection des données doivent être adaptées aux processus établis dans l'environnement en fonction des besoins de protection des données.

[17] Le Regulator décide de la façon dont l'obligation d'information est remplie. Les utilisateurs ont aussi le droit de savoir comment les données personnelles sont utilisées et peuvent en faire la demande avant que les données soient recueillies.

10 Modèles d'Identity Federation

La topologie d'un système d'*Identity Federation* décrit l'agencement des différents composants et leurs relations logiques. En fonction des conditions générales et des exigences, on distingue quatre agencements différents, qui font l'objet de brèves descriptions dans les sections suivantes.

10.1 Modèle centré sur le RP

Le *modèle centré sur le RP* est illustré par la Figure 25. Ce modèle présente l'avantage pour le *Relying Party (RP)* de ne pas devoir gérer lui-même les *E-Identities* en pouvant déléguer l'authentification du sujet à l'un des IdP dignes de confiance.

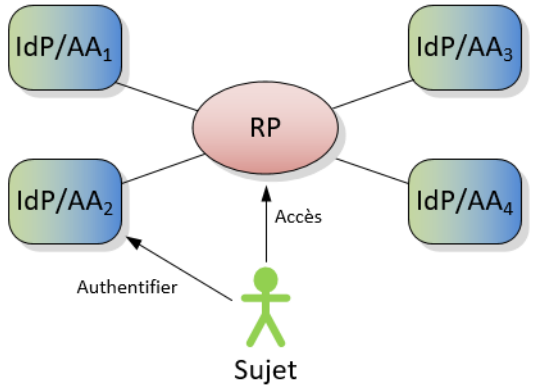


Figure 25 Modèle centré sur le RP

10.2 Modèle centré sur l'IdP

Autre scénario typique, le *modèle centré sur l'IdP* (voir Figure 26). Ce modèle consiste pour un *sujet* à s'authentifier auprès d'un *IdP/AP* central (son organisation d'origine par exemple) afin d'utiliser la confirmation d'authentification dans un souci de transparence d'*accès* à différents *RP*.

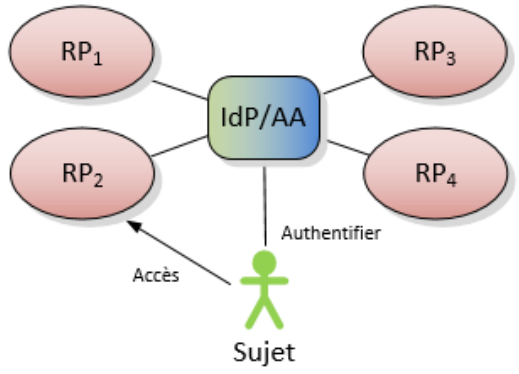


Figure 26 Modèle centré sur l'IdP

10.3 Modèle Full-meshed

La Figure 27 présente la façon dont, dans un modèle *full-meshed,* plusieurs organisations fédèrent mutuellement les identités par-delà les limites de ces organisations. Dans un modèle *full-meshed,* chaque organisation échange les informations nécessaires de leurs propres systèmes avec les organisations partenaires.

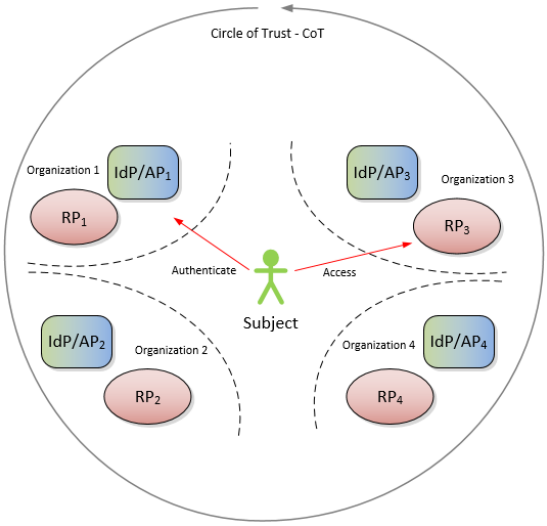


Figure 27: Modèle Full-meshed

10.4 Modèle Hub-'n'-Spoke

Un modèle Hub-'n'-Spoke[18] repose sur une infrastructure centrale d'intermédiaire - le *Broker*. Toutes les parties impliquées font confiance à ce *Broker*. Comme en témoigne la Figure 28, les fournisseurs (*IdP/AP*) et consommateurs (*RP*) d'identité ne communiquent plus directement l'un avec l'autre. Ils échangent leurs messages via le *Broker*, qui les contrôle et les transmet au bon destinataire.

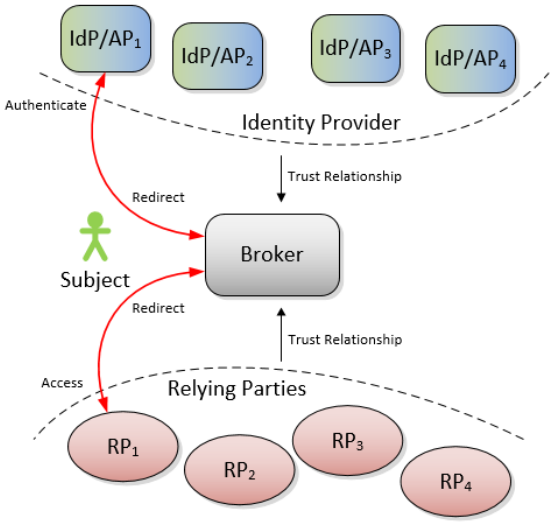


Figure 28: Modèle Hub-'n'-Spoke

[18] Moyeu et rayon de roue

11 Exclusion de responsabilité - droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisateurs, ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association **eCH** ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes **eCH** ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes **eCH** peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association **eCH** mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes **eCH** peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des réglementations applicables.

12 Droits d'auteur

Tout auteur de normes **eCH** en conserve la propriété intellectuelle. Il s’engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu’à l’association **eCH**, pour une utilisation et un développement sans restriction dans le cadre des buts de l’association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes **eCH** sont complètement documentées et libres de toute restriction relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s’appliquent exclusivement aux normes élaborées par **eCH**, non aux normes ou produits de tiers auxquels il est fait référence dans les normes **eCH**. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Références & bibliographie

[1] A. Laube-rosenpflanzer, A. Spichiger, T. Kessler, A. Müller, and M. Kunz, “eCH-0219 - IAM-Glossar,” vol. 1.0, 2017.

[2] W. Müller and H. Lindner, “eCH-0122 – Architektur E-Government Schweiz : Grundlagen Dokument,” vol. 1.0, pp. 1–26, 2014 [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0122

[3] Wikipedia, “IT Infrastructure Library.” [Online]. Available: https://de.wikipedia.org/wiki/IT_Infrastructure_Library

[4] “Protokoll Expertenworkshop ‘Sicherheitsopportunitäten für den Wirtschaftsstandort Schweiz’ vom 8.11.2012 (zu Strategie Informationsgesellschaft),” 2012.

[5] M. Topfel, T. Jarchow, A. Spichiger, and R. Bernold, “eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID,” vol. 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=a26d17d1-fe03-4226-97ab-9beefef22856

[6] International Standards Organisation, “ISO 31000 - Risk management,” *ISO 31000:2009 - Risk Management*. p. 1, 2009 [Online]. Available: http://www.iso.org/iso/home/standards/iso31000.htm

[7] ISACA, *COBIT 5 Framework*. 2012 [Online]. Available: www.isaca.org/COBIT

[8] P. Editors, W. Fumy, M. De Soete, E. J. Humphreys, K. Naemura, and K. Rannenberg, “ITU-T Recommendation X . 1254 | International Standard ISO / IEC DIS 29115 Information technology — Security techniques — Entity authentication assurance framework,” 2011.

[9] Union européenne, “Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015,” no. septembre, 2012.

[10] H. Häni and U. Kienholz, “eCH-0172 IAM-Maturitätsmodell,” vol. 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=a26d17d1-fe03-4226-97ab-9beefef22856

[11] A. Laube-Rosenpflanzer, G. Hassenstein, M. Kunz, T. Gruoner, A. Spichiger, and T. Selzam, “eCH-0170 Qualitätsmodell zur Authentifizierung von Sujeten,” vol. 2.0, 2017 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=54cce841-215f-4887-9382-25620dcbf9b1

[12] ISO/IEC, “ISO/IEC 27001:2013” [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[13] A. Laube-rosenpflanzer, G. Hassenstein, S. Agosti, M. Vinzens, U. Pfenninger, and D. Leiser, “eCH-0168 SuisseTrustIAM technische Architektur und Processus,” vol. 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=31499686-813d-4589-b794-11015fbf2059

[14] A. Laube-rosenpflanzer and G. Hassenstein, “eCH-0174 SuisseTrustIAM - Implementierung mit SAML 2.0,” vol. 1.0, 2015 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=5d8ee101-aba3-4061-aba0-aaed23b1f04f

Annexe B – Collaboration & vérification

Gruoner Torsten	UPIC
Hassenstein Gerhard	Haute école spécialisée bernoise, TI
Heerkens Marc	UPIC
Hefti Esther	Chancellerie cantonale de Zurich
Kessler Thomas	Temet
Kunz Marc	Haute école spécialisée bernoise, TI
Laube-Rosenpflanzer Annett	Haute école spécialisée bernoise, TI
Leimer Bojan	Haute école spécialisée bernoise, TI
Spichiger Andreas	Haute école spécialisée bernoise, FBW
	Groupe spécialisé eCH IAM

V2.0:
Ronny Bernold, BFH FBW, ronny.bernold@bfh.ch
Gerhard Hassenstein, BFH TI, gerhard.hassenstein@bfh.ch
Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch
Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch
Martin Topfel, BFH FBW, martin.topfel@bfh.ch
eCH Fachgruppe IAM

V1.0:
Willy Müller, ISB, willy.mueller@isb.admin.ch
Hans Häni, AFT TG

Annexe C – Abréviations

AP	Attribute Provider
C2G	Citizen to Government
CP	Credential Provider
CSP	Credential Service Provider
eIDAS	electronic IDentification, Authentication and trust Services
IAM	Identity und Access Management
IdP	Identity Provider
IoT	Internet of Things
ISMS	Système de gestion de la sécurité des informations
ITIL	IT-Service-Management
LB	Bénéficiaire de prestations
LE	Fournisseur de prestations
OIDC	OpenID Connect
PIN	Personal Identification Number
PUF	Physical Unclonalbe Function
RA	Service d'inscription / Registration Authority
RP	Relying Party
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SoD	Segregation of Duties
SSO	Single Sign-On
TLS	Transport Layer Security
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Annexe D – Glossaire

La terminologie utilisée dans cette norme provient exclusivement de la norme eCH eCH-0219 V1.0 [1].

Annexe E – Modifications par rapport à la version 2.00

La présente norme est basée sur les principes opérationnels de l'eCH-0107 v2.00. La version remaniée comporte cependant de nouveaux concepts et connaissances fondamentaux.

La version 3.0 de l'eCH-0107 a été en grande partie remaniée.

Les modifications générales sont énumérées ci-dessous et renvoient au contenu de la version 2.00 de l'eCH-0107.

Modifications principales:

- *La structure des chapitres n'a pas fait l'objet d'une refonte majeure, seules quelques sections ont été remaniées.*
- *V2.0 se limite en conséquence à l'IAM inter-organisations.*

Le glossaire de la V2.0 contient de nombreux termes du domaine IAM, mais qui n'ont pas été utilisés dans le document. Ce glossaire a été déplacé dans une norme dédiée (eCH-0219 [1]) afin de pouvoir utiliser à l'avenir une terminologie pour toutes les normes IAM. Le document à proprement parler ne mentionne que les termes utilisés nécessaires à la compréhension.

Fehler! Verweisquelle konnte nicht gefunden werden. **[eCH-0107 V2.0 Chapitre 2]**

- *L'introduction a fait l'objet d'une refonte complète et se concentre sur un IAM fédéré dans un contexte inter-organisations.*

Chapitre Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden. **[eCH-0107 V2.0 Chapitre 3]**

- *On distingue désormais les Stakeholders des acteurs dans l'IAM; alors que les Stakeholders décrivent les aspects de motivation, les différents acteurs sont les exécutants des processus du chapitre 6. Les relations entre Stakeholders et acteurs sont décrites.*

Chapitre 4 Exigences

- *Les principes de conception et les exigences générales imposées à un système IAM fédéré ont été remaniés et complétés de nouveaux constats (tirés de eCH-0168* [13], *eCH-0174* [14], *eCH-0170* [11] *par exemple*). *Ils ont été restructurés, classés et justifiés.*
- *Les exigences des différents Stakeholders ont été remaniées, élargies, justifiées.*

Chapitre Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden. **[eCH-0107 v2.00 Chapitre 5]**

- *Le modèle d'information a été élargi. Ce faisant, les compléments issus de la norme eCH-0170* [11] *ont été repris et intégrés au modèle en question.*
- *Un autre complément porte sur le sujet, qui englobe désormais également les* ***choses****, ainsi que sur la distinction entre les organisations qui agissent et celles qui n'agissent pas. La délégation des droits a elle aussi été retravaillée.*

Chapitre Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden. **[eCH-0107 v2.00 Chapitre 5]**

- *Les processus ont été mis à jour, complétés et matérialisés. Les processus sont désormais divisés plus finement et les processus d'appui ont été ajoutés (chapitre 6.5). Tous les processus ont été motivés par les exigences du chapitre* ***Fehler! Verweisquelle konnte nicht gefunden werden.****.*

Chapitre Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden. **[eCH-0107 v2.00 Chapitre 6]**

- *Les services administratifs ont été renommés services IAM*
- *Les services IAM ont été nettement remaniés et adaptés à l'IAM fédéré.*
- *Les interfaces pour tous les services IAM ont été définies.*
- *Les services IAM ont été affectés à un processus chacun.*
- *Le chapitre 7.5 a été entièrement remaniée sur la base de la mise à jour des processus à la section 6.1.*

Chapitre 8 IAM pour l'IoT [nouveau]

- *Ce chapitre traite des exigences et répercussions de l'IoT sur les principes de conception de la gestion des identités et des accès (IAM).*

Chapitre Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden. **[nouveau]**

- Ce chapitre décrit les exigences relatives à la protection de la vie privée du sujet et les directives de gestion et de traitement des données du sujet.

Chapitre Fehler! Verweisquelle konnte nicht gefunden werden. **Modèle Identity Federation [eCH-0107 v2.00 Chapitre 6]**

- Les illustrations du chapitre ont été adaptées. Les descriptions ont fait l'objet d'une mise à jour minimale.

Annexe F – Liste des figures

Annexe G – Liste des tableaux